Departamento de Matemáticas
Universidad Autónoma de Madrid

Sets of integers with additive restrictions

Memoria de Tesis Doctoral presentada por

Rafael Tesoro Carretero

para optar al título de Doctor en Ciencias Matemáticas
Programa de Doctorado de Matemáticas

Trabajo supervisado por

Javier Cilleruelo Mateo
Profesor Titular del Departamento de Matemáticas
Universidad Autónoma de Madrid

Noviembre de 2015

"[...]
Bien está el resignado aprendizaje
De una empresa infinita; yo he elegido
El de tu lengua, ese latín del Norte
Que abarcó las estepas y los mares
De un hemisferio y resonó en Bizancio
Y en las márgenes vírgenes de América.
Sé que no lo sabré, pero me esperan
Los eventuales dones de la busca,
No el fruto sabiamente inalcanzable.
Lo mismo sentirán quienes indagan
Los astros o la serie de los números...
[...] "

Tomado del poema *A Islandia* de Jorge Luis Borges.

Gracias

Michael Atiyah dijo sobre la creación en matemáticas: "El camino más corto para crear es un largo rodeo." Libraré al lector de un largo prólogo sobre el rodeo, esforzado y a la vez placentero, que me ha traído hasta aquí.

Gracias a los profesores que encendieron las chispas del matemático que llevo dentro. El primero de ellos lo encontré en el instituto y sus clases me llevaron a la Universidad Autónoma de Madrid. Gracias a tantas personas que he encontrado en mi largo rodeo: en el Departamento de Matemáticas, en el Instituto de Ciencias Matemáticas, en varios congresos como el Erdős Centennial del año 2013.

Mi mayor agradecimiento es para Javier Cilleruelo. Compañeros de estudios de licenciatura, pronto nos hicimos amigos. En esta última etapa, Javier aceptó supervisar mi trabajo de estudiante de doctorado. Desde este punto en que ya diviso la meta, recuerdo su infatigable apoyo que me ha acompañado y orientado en el camino. Termino con el recuerdo del agradable sonido de la guitarra tañida por sus dedos, los mismos dedos que vienen desde hace tiempo redactando con esmero bellos textos matemáticos.

> "Trabaja mucho primero y diviértete mucho después. Las grandes ideas llegarán cuando estés relajado. Pero ni antes ni después te fuerces a conseguir nada por obligación: hazlo todo por ilusión y los problemas más difíciles se convertirán en divertidos juegos. Esfuérzate, pero no te fuerces ni te estreses ni te dejes presionar: la creatividad siempre llega del brazo de la libertad."[1]

Bruselas, noviembre de 2015.

[1] Entrevista a Michael Atiyah `http://www.lavanguardia.com/lacontra/20111228/54241694041/sir-michael-atiyah-el-camino-mas-corto-para-crear-es-un-largo-rodeo.html`

Contents

List of Figures

Notation

We will denote by $|A|$ the cardinal or size of a finite set A and by $|\mathfrak{p}|$ the modulus of a complex number $\mathfrak{p}$.

We will indifferently use the notation of Landau $f = O(g)$ and the notation of Vinogradov $f \ll g$ to mean that there exists an implicit constant $C > 0$ such that $|f| \le C|g|$ in all the range of f. The expression $f \gg g$ will just mean that $g \ll f$, and $f \asymp g$ will mean that both $f \ll g$ and $f \gg g$ are true. As an example we will write

$$|S_m| \gg 4^{m\left(1-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}-\epsilon\right)}, \quad (m \to \infty),$$

to mean that there exist $C > 0$ such that $|S_m| \ge C \cdot 4^{m\left(1-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}-\epsilon\right)}$ holds for all m sufficiently large.

We will write $f \sim g$ if $(f/g)(x) \overset{x\to\infty}{\longrightarrow} 1$, and $f = o(g)$ if $(f/g)(x) \overset{x\to\infty}{\longrightarrow} 0$.

The integer inferior part and the integer superior part of a number x will be denoted by $\lfloor x \rfloor$ and $\lceil x \rceil$ respectively. The distance from x to $\mathbb{Z}$ will be denoted by $\|x\| = \min_{n\in\mathbb{Z}} |x-n|$.

To confirm the exact meaning of other symbols used in this work please refer to the corresponding definition as indicated in the following table.

Symbol	**Meaning**	**For definition refer to**
$A(x)$	Counting function of a sequence.	page 18
$\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free	Free of sumsets with summands of prescribed size.	Definition 2.1 in page 20
$\mathcal{L}$-free	Generic mention to any $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free.	
$F(n, \mathcal{L}_{\ell_1,\dots,\ell_r})$	Extremal size of $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set in $\{1,\dots,n\}$.	page 22
$F(G, \mathcal{L}_{\ell_1,\dots,\ell_r})$	Extremal size of $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set in G.	page 24
$\mathrm{ex}(n, \mathcal{H})$	Extremal number of edges in a graph avoiding $\mathcal{H}$.	page 25
$K^{(r)}_{\ell_1,\dots,\ell_r}$	r-uniform hypergraph.	Definition 2.4 in page 25
$f(n, P, d)$	Extremal number of ones in a matrix avoiding P.	Definition 2.5 in page 27

Resumen y conclusiones

El presente trabajo se centra en el estudio de conjuntos finitos y sucesiones infinitas de enteros positivos con ciertas restricciones aritméticas de carácter aditivo. En el capítulo 1 estudiamos sucesiones de enteros donde todas las sumas de h elementos de la sucesión son distintas. Estas sucesiones se denominan sucesiones B_h. En el capítulo 2 estudiamos sucesiones de enteros que no contienen conjuntos suma $L_1 + \cdots + L_r$ donde los tamaños de los sumandos están fijados, $|L_i| = \ell_i,\ i = 1, \dots, r$. A estas sucesiones las llamaremos sucesiones $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-libres, y de manera genérica sucesiones $\mathcal{L}$-libres. Estudiamos también conjuntos finitos $\mathcal{L}$-libres en intervalos de enteros y en grupos abelianos finitos.

Tanto las sucesiones B_h como las sucesiones $\mathcal{L}$-libres son generalizaciones naturales de las sucesiones de Sidon, introducidas por Erdős. Las sucesiones de Sidon son aquellas sucesiones de enteros tales que todas las diferencias no nulas de dos de sus elementos son distintas. Tanto las sucesiones B_2 como las sucesiones $\mathcal{L}_{2,2}$-libres coinciden precisamente con las sucesiones de Sidon.

Si bien es fácil construir sucesiones con este tipo de restricciones, el reto consiste en construirlas con la mayor densidad posible. Es natural pesar que cuanto más densa sea una sucesión más difícil resulta que dicha sucesión satisfaga una restricción de las mencionadas anteriormente. Construir sucesiones densas con las restricciones mencionadas y obtener cotas sucesiones para estas densidades son los objetivos centrales de este trabajo. También estudiamos los problemas análogos en el caso de conjuntos finitos $\mathcal{L}$-libres.

Sucesiones con otras restricciones aditivas han sido estudiadas en la literatura, siendo las más populares aquellas sucesiones que evitan progresiones aritméticas de longitud k. El teorema de Szemerédi, central en este área, afirma que dichas sucesiones tienen densidad 0 para todo $k \geq 3$.

Hay un último capítulo dedicado a los números palindrómicos en la sucesión de Fibonacci, que nada tiene que ver con el tema principal de la tesis pero que ha formado parte de mi trabajo durante mi periodo como estudiante de doctorado.

Sucesiones B_h densas

Sea $h \geq 2$ un entero. Decimos que una sucesión $\mathcal{B}$ de enteros positivos es una sucesión B_h si todas las sumas

$$b_1 + \cdots + b_h, \qquad (b_k \in \mathcal{B},\ 1 \leq k \leq h),$$

son distintas, con la condición de que $b_1 \leq b_2 \leq \cdots \leq b_h$. Del mismo modo se pueden definir los conjuntos finitos B_h.

Los conjuntos B_2 y las sucesiones B_2 son habitualmente conocidas como conjuntos de Sidon y sucesiones de Sidon respectivamente. En este caso particular, la restricción aritmética de que todas las sumas $b_1+b_2,\ (b_k \in \mathcal{B},\ b_1 \leq b_2)$, sean distintas es equivalente a pedir que la sucesión $\mathcal{B}$ no contenga cuatro elementos dispuestos como se muestra a continuación:

Figura 1: Disposición prohibida en sucesiones/conjuntos de Sidon.

La razón es que si una sucesión contuviese cuatro elementos dispuestos como en la figura 1 tendría dos pares distintos de elementos $\{b_1, b_1'\}, \{b_2', b_2\}$ tales que $b_1' - b_1 = b_2 - b_2'$, es decir $b_1 + b_2 = b_1' + b_2'$, con $\{b_1, b_2\} \neq \{b_1', b_2'\}$. Por tanto, las sucesiones B_2 se caracterizan por evitar la disposición de la figura 1.

Dada una sucesión infinita de enteros A cualquiera, su *función contadora* se define como $A(x) = \{a \in A\colon a \leq x\}$. El estudio de la función contadora de las sucesiones infinitas B_h (o del tamaño de los conjuntos finitos B_h) es un tema clásico en la teoría combinatoria de números. Unas cuentas sencillas prueban que si $\mathcal{B} \subset \{1, \cdots, n\}$ es un conjunto B_h entonces $|\mathcal{B}| \leq (C_h + o(1))n^{1/h}$ para una constante C_h (v. [9] y [26] para cotas superiores no triviales de C_h) y en consecuencia tenemos que $\mathcal{B}(x) \ll x^{1/h}$ cuando $\mathcal{B}$ es una sucesión infinita B_h.

Erdős conjeturó la existencia, para todo $\epsilon > 0$, de una sucesión $\mathcal{B}$ infinita B_h con función contadora $\mathcal{B}(x) \gg x^{1/h-\epsilon}$. Se cree que no podemos quitar ϵ de este último exponente, un hecho que sólo se ha probado para h par. El algoritmo *avaricioso* produce una sucesión B_h infinita $\mathcal{B}$ con

$$\mathcal{B}(x) \gg x^{\frac{1}{2h-1}} \quad (h \geq 2). \tag{0.1}$$

Para el caso $h = 2$, Atjai, Komlós and Szemerédi [1] demostraron que existe una sucesión B_2 con $\mathcal{B}(x) \gg (x \log x)^{1/3}$, mejorando en una potencia de logaritmo la cota inferior (0.1). El mayor avance sobre (0.1) para el caso $h = 2$ fue logrado por Ruzsa [42], quien construyó de una manera ingeniosa una sucesión infinita de Sidon $\mathcal{B}$ satisfaciendo

$$\mathcal{B}(x) = x^{\sqrt{2}-1+o(1)}. \tag{0.2}$$

En el capítulo 1 adaptamos las ideas de Ruzsa para construir sucesiones infinitas densas B_3 y B_4 que mejoran, por primera vez, la cota inferior (0.1) para $h = 3$ y $h = 4$.

Teorema 1.1 *Para $h = 2, 3, 4$ existe un sucesión $\mathcal{B}$ infinita B_h con función contadora*

$$\mathcal{B}(x) = x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}.$$

Después de nuestro trabajo en esta materia [13], Cilleruelo [8] obtuvo la misma estimación (0.2) para la función contadora de sucesiones infinitas de Sidon utilizando una construcción diferente de la de Ruzsa. Además Cilleruelo adaptó su construcción para demostrar el teorema 1.1 para todo $h \geq 2$.

Conjuntos y sucesiones $\mathcal{L}$-libres

Los conjuntos y las sucesiones B_h son una de las posibles generalizaciones de los conjuntos y las sucesiones de Sidon. En el capítulo 2 estudiamos problemas extremales en el contexto de otra generalización natural de los conjuntos y las sucesiones de Sidon. También mostramos las conexiones de dichos problemas con ciertos problemas extremales en grafos e hipergrafos y con ciertos problemas extremales en matrices.

La definición principal para toda la segunda parte de este trabajo es el concepto siguiente, al que nos referiremos usando la expresión genérica *"$\mathcal{L}$-libre"*:

Definición 2.1 *Sean $r, \ell_1, \dots, \ell_r$ enteros con $r \geq 1$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$. Dado un grupo abeliano G decimos que $A \subset G$ es un conjunto $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-libre si A no contiene ningún conjunto-suma de la forma*

$$L_1 + \cdots + L_r = \{\lambda_1 + \cdots + \lambda_r : \ \lambda_i \in L_i, \ i = 1, \dots, r\},$$

con $|L_i| = \ell_i, \ i = 1, \dots, r$. Para $r = 2$ escribimos simplemente $\mathcal{L}_{\ell_1,\ell_2}$.

Como es habitual en la literatura matemática llamamos *conjunto-suma* a $L_1 + \cdots + L_r$.

En el capítulo 2 estudiamos los conjuntos finitos $\mathcal{L}$-libres y las sucesiones infinitas $\mathcal{L}$-libres, es decir, con la restricción de estar libres de conjuntos-suma con sumandos de tamaño preestablecido.

Para motivar la definición 2.1 recordamos varios casos particulares de esta restricción aritmética, que han sido estudiados ya en la literatura.

1. *Conjuntos $\mathcal{L}_{2,2}$-libres.* Podemos representar un conjunto-suma con sumandos de 2 elementos $L_1 + L_2$, como dos copias de un par de puntos:

   

   Cada punto representa una suma en $L_1 + L_2$. Esta es la misma disposición que la de la figura 1. Está claro que cualquier conjunto que contuviese esta disposición de cuatro puntos contendría dos parejas distintas de elementos con la misma distancia entre cada pareja. Dicho de otro modo: los conjuntos de Sidon son precisamente los conjuntos $\mathcal{L}_{2,2}$-libres.

2. *Conjuntos $\mathcal{L}_{2,\ell}$-libres.* Un conjunto $\mathcal{L}_{2,\ell}$-libre A se caracteriza por la propiedad de cualquier elemento del grupo ambiente se puede expresar a lo sumo de $\ell-1$ maneras diferentes como la diferencia de dos elementos de A. Estos conjuntos han sido denominados conjuntos $B_2^{\circ}[\ell-1]$ [32] y también conjuntos $B_2^{-}[\ell-1]$ [45].

   Por ejemplo, el aspecto típico de un conjunto-suma L_1+L_2 con $|L_1|=2$ y $|L_2|=3$ es el de tres copias de un par de puntos:

Figura 2: Disposición prohibida en sucesiones/conjuntos $\mathcal{L}_{2,3}$-libres.

   Los conjuntos $\mathcal{L}_{2,3}$-libres se caracterizan por estar libres de disposiciones de seis elementos como la de la figura 2.

3. *Conjuntos $\mathcal{L}_{\ell_1,\ell_2}$-libres.* Los conjuntos que no contienen ℓ_2 copias de conjuntos con ℓ_1 elementos fueron introducidos por Erdős and Harzheim [18] y después estudiados en [40]. Por ejemplo los conjuntos $\mathcal{L}_{3,4}$-libres se caracterizan por evitar cuatro copias de tres puntos, una disposición que podemos representar así:

Figura 3: Disposición prohibida en sucesiones/conjuntos $\mathcal{L}_{3,4}$-libres.

4. *Conjuntos $\mathcal{L}^{(r)}_{2,\dots,2}$-libres* Un cubo de Hilbert de dimensión r es un conjunto suma $L_1+\cdots+L_r$, con $|L_1|=\cdots=|L_r|=2$. Por tanto, los conjuntos $\mathcal{L}^{(r)}_{2,\dots,2}$-libres son aquellos que están libres de cubos de Hilbert de dimensión r. Un cubo de Hilbert de dimensión 3 tiene este aspecto:

Figura 4: Cubo de Hilbert de dimensión 3, prohibido en $\mathcal{L}_{2,2,2}$-libres.

> Primero se copian dos veces un par de puntos, en la parte izquierda de la figura 4 (esta parte es idéntica a la figura 1). A continuación se copia esta parte izquierda en la derecha de la página, y obtenemos finalmente los 8 puntos de un cubo de Hilbert de dimensión 3.

Nótese que algunas de las sumas en $L_1 + \cdots + L_r$ podrían repetirse y en estos casos (que llamaremos degenerados), las representaciones de las sumas contendrían menos puntos de los que hemos dibujado. Por ejemplo: el conjunto-suma $\{2,3\} + \{1,2\} = \{3,4,5\}$ tiene tres elementos, en lugar de cuatro, y se puede representar así:

Figura 5: Otra disposición prohibida en sucesiones/conjuntos de Sidon.

Cualquier sucesión que contenga $\{3,4,5\}$ no es de Sidon pues, aunque evitase la disposición de la figura 1, no puede evitar la disposición de la figura 5.

Conjuntos finitos y $\mathcal{L}$-libres extremales

En §2.1.1 y en §2.3 estudiamos conjuntos finitos y $\mathcal{L}$-libres dentro del intervalo $\{1,\dots,n\}$ y en grupos abelianos finitos. Nuestros principales resultados se resumen a continuación.

Llamemos $F\big(n, \mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}\big)$ al tamaño de los conjuntos $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-libres más grandes en el intervalo $\{1,\dots,n\}$. La cota superior para el caso general que hemos conseguido recupera las cotas superiores ya conocidas para los casos particulares que hemos recordado en las páginas anteriores.

Teorema 2.1 *Para cualesquiera $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$, tenemos*

$$F\big(n, \mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}\big) \leq (\ell_r - 1)^{\frac{1}{\ell_1\cdots\ell_{r-1}}} n^{1-\frac{1}{\ell_1\cdots\ell_{r-1}}} + O\left(n^{\frac{1}{2}+\frac{1}{2\ell_{r-1}}-\frac{1}{\ell_1\cdots\ell_{r-1}}}\right).$$

A continuación comparamos el teorema 2.1 con las cotas superiores que se conocen para algunos los casos particulares ya mencionados:

i) *Conjuntos $\mathcal{L}_{2,2}$-libres.* Erdős y Turán [22] obtuvieron la cota superior $|A| \leq \sqrt{n} + O(n^{1/4})$ para cualquier conjunto de Sidon $A \subset \{1, \ldots, n\}$, estimación que fue después refinada hasta $|A| < \sqrt{n} + n^{1/4} + 1/2$ por otros autores [33, 41, 10]. La estimación de Erdős-Turán se deduce del teorema 2.1 para $r = \ell_1 = \ell_2 = 2$.

ii) *Conjuntos $\mathcal{L}_{2,\ell}$-libres.* La cota superior $|A| < \sqrt{(\ell-1)n} + ((\ell-1)n)^{1/4} + 1/2$ para un conjunto A que sea $B_2^\circ[\ell-1]$, con $A \subset \{1, \ldots, n\}$, fue obtenida en [10]. El teorema 2.1 para $r = \ell_1 = 2$ y $\ell_2 = \ell \geq 2$ nos da

$$F(n, \mathcal{L}_{2,\ell}) \leq (\ell-1)^{1/2} n^{1/2} + O(n^{\frac{1}{4}}).$$

iii) *Conjuntos $\mathcal{L}_{\ell_1,\ell_2}$-libres.* Peng, Tesoro y Timmons [40] demostraron que si $A \subset \{1, \ldots, n\}$ no contiene ℓ_1 copias de ningún conjunto de ℓ_2 elementos, entonces $|A| \leq (\ell_2 - 1)^{1/\ell_1} n^{1-1/\ell_1} + O\left(n^{1/2-1/(2\ell_1)}\right)$. Esto también se deduce del teorema 2.1 para $r = 2$. Nótese que Erdős y Harzheim [18] habían obtenido previamente la estimación más débil $|A| \ll n^{1-1/\ell_1}$ para estos conjuntos.

iv) *Conjuntos $\mathcal{L}^{(r)}_{2,\ldots,2}$-libres.* Csaba Sándor [43] probó que si $A \subset \{1, \ldots, n\}$ no contiene un cubo de Hilbert de dimensión r entonces $|A| \leq n^{1-1/2^{r-1}} + 2n^{1-1/2^{r-2}}$, excepto para una cantidad finita de n. El teorema 2.1 en el caso $\mathcal{L}^{(r)}_{2,\ldots,2}$ implica

$$F(n, \mathcal{L}^{(r)}_{2,\ldots,2}) \leq n^{1-1/2^{r-1}} + O\left(n^{3/4-1/2^{r-1}}\right),$$

lo cual mejora el término de error para $r \geq 4$ en la estimación de Sándor.

En la otra dirección, usando el método probabilístico, obtenemos una cota inferior para el caso general.

Teorema 2.2 *Para cualesquiera $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$, tenemos*

$$F(n, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}) \geq n^{1-\frac{\ell_1+\cdots+\ell_r \; -r}{\ell_1\cdots\ell_r \; -1} - o(1)}.$$

Los exponentes en estas cotas inferior y superior son distintos y el reto es reducir la distancia que los separa. Creemos que el exponente para los conjuntos extremales $\mathcal{L}$-libres en intervalos es el conseguido en la cota superior:

Conjetura 2.1 *Para cualesquiera $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$, tenemos*

$$F(n, \mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r}) \asymp n^{1-1/(\ell_1\cdots\ell_{r-1})}.$$

Esta conjetura se sabe cierta para el caso $r = \ell_1 = 2$:

$$F(n, \mathcal{L}_{2,\ell_2}) \sim (\ell_2 - 1)^{1/2} n^{1-1/2}, \quad (\ell_2 \geq 2).$$

Esta última asintótica para el caso particular $\ell_2 = 2$ recupera la estimación de Erdős y Turán [22] para conjuntos extremales de Sidon y fue generalizada por Trujillo-Solarte, García-Pulgarín y Velásquez-Soto [45]. Nosotros hemos probado la conjetura 2.1 en dos casos más:

$$\begin{aligned} F(n, \mathcal{L}_{3,\ell_2}) &\asymp n^{1-1/3}, \quad (\ell_2 \geq 3), \\ F(n, \mathcal{L}_{\ell_1,\ell_2}) &\asymp n^{1-1/\ell_1}, \quad (\ell_2 \geq \ell_1! + 1). \end{aligned}$$

Estos dos casos son consecuencias inmediatas del teorema 2.3 y del teorema 2.4 respectivamente.

Teorema 2.3 *Para cualquier entero $n \geq 1$, existe un conjunto $\mathcal{L}_{3,3}$-libre $A \subset \{1, \ldots, n\}$ con*

$$|A| \geq \left(4^{-2/3} + o(1)\right) n^{2/3}.$$

Teorema 2.4 *Sea $\ell \geq 2$ un entero. Para cualquier entero $n \geq 1$, existe un conjunto $\mathcal{L}_{\ell,\ell!+1}$-libre $A \subset \{1, \ldots, n\}$ con*

$$|A| = (1 + o(1)) \left(\frac{n}{2^{\ell-1}}\right)^{1-1/\ell}.$$

En §2.1.1 estudiamos también conjuntos extremales $\mathcal{L}$-libres contenidos en un grupo abeliano finito G. Llamaremos $F(G, \mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r})$ al tamaño máximo de un conjunto $\mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r}$-libre en G.

Hemos obtenido la siguiente cota superior para el tamaño de subconjuntos de $\mathbb{Z}^3_{p-1}$ que no contienen cubos de Hilbert de dimensión 3:

Teorema 2.5 *Para cualquier primo $p \geq 2$ tenemos*

$$F(\mathbb{Z}_{p-1}^3, \mathcal{L}_{2,2,2}^{(3)}) \geq (p-3)^2.$$

Como consecuencia del teorema 2.5 confirmamos, con una construcción diferente, la cota inferior

$$F(n, \mathcal{L}_{2,2,2}^{(3)}) \gg n^{1-1/3},$$

que fue obtenida por Katz, Krop and Maggioni [29]. Esta estimación mejora la cota inferior $F(n, \mathcal{L}_{2,2,2}^{(3)}) \gg n^{1-3/7-o(1)}$ que nos da el teorema 2.2.

El tamaño extremal en intervalos y el tamaño extremal en grupos finitos se relacionan como sigue:

Proposición 2.1 *Para cualesquiera $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$, y $n_1, \cdots, n_k$, tenemos*

$$F(2^{k-1} n_1 \cdots n_k, \mathcal{L}_{\ell_1,\ldots,\ell_r}^{(r)}) \geq F(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, \mathcal{L}_{\ell_1,\ldots,\ell_r}^{(r)}).$$

Conexiones con problemas extremales en grafos

Dado un grafo (o hipergrafo) $\mathcal{H}$, denotemos por $\mathrm{ex}(n, \mathcal{H})$ el máximo número de aristas (o hiperaristas) de un grafo (o hipergrafo) de n vértices que no contenga $\mathcal{H}$ como un sub-grafo (o sub-hipergrafo). Estimar $\mathrm{ex}(n, \mathcal{H})$ es un problema importante en teoría extremal de grafos.

En §2.1.2, §2.1.3, §2.4.1 y §2.4.2 presentamos y demostramos conexiones entre los problemas en $\mathcal{L}$-libres y el problema de Turán en grafos e hipergrafos. Para resumir dichas conexiones, vamos a definir primero el hipergrafo r-uniforme.

Definición 2.4 *Sean $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$ enteros. Denominamos $K_{\ell_1,\ldots,\ell_r}^{(r)}$ al hipergrafo r-uniforme $(V, \mathcal{E})$ donde $V = V_1 \cup \cdots \cup V_r$ con $|V_i| = \ell_i$, $i = 1, \ldots, r$ y*

$$\mathcal{E} = \{\{x_1, \ldots, x_r\} : \ x_i \in V_i, \ i = 1, \ldots, r\}.$$

Diremos que el r-hipergrafo $\mathcal{G}$ es $K^{(r)}_{\ell_1,\dots,\ell_r}$-libre cuando $\mathcal{G}$ no contiene ningún hipergrafo r-uniforme $K^{(r)}_{\ell_1,\dots,\ell_r}$.

Un argumento probabilístico sencillo da la siguiente cota inferior:

$$n^{r-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}} \ll \mathrm{ex}(n; K^{(r)}_{\ell_1,\cdots,\ell_r}). \tag{0.3}$$

Erdős consideró la cota superior para el caso $\ell = \ell_1 = \cdots = \ell_r$, y demostró [17, teorema 1] que

$$ex(n, K^{(r)}_{\ell,\dots,\ell}) \ll n^{r-1/\ell^{r-1}}. \tag{0.4}$$

Nosotros hemos refinado y generalizado la estimación (0.4) como sigue.

Teorema 2.6 *Para cualesquiera $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$, tenemos*

$$ex(n, K^{(r)}_{\ell_1,\dots,\ell_r}) \leq \frac{(\ell_r - 1)^{1/\ell_1\cdots\ell_{r-1}}}{r!}\, n^{r-1/\ell_1\cdots\ell_{r-1}}(1+o(1)), \quad (n \to \infty). \tag{0.5}$$

El caso $r = 2$ en el teorema 2.6 fue demostrado por Kövari, Sós y Turán [31]. Se cree que la cota superior en (0.5) no está lejos del valor real de $ex(n, K^{(r)}_{\ell_1,\dots,\ell_r})$.

Conjetura 2.2 *Para cualesquiera $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$, tenemos*

$$ex(n, K^{(r)}_{\ell_1,\cdots,\ell_r}) \asymp n^{r-1/\ell_1\cdots\ell_{r-1}}.$$

Los dos exponentes de n en los teoremas 2.1 y 2.2 y los que aparecen en (0.3) y en (0.5) tienen una forma similar. El siguiente resultado explica esta similitud:

Proposición 2.2 *Sea G un grupo abeliano finito con $|G| = n$. Para cualesquiera $r \geq 2$ y $2 \leq \ell_1 \leq \cdots \leq \ell_r$, tenemos*

$$ex(n, K^{(r)}_{\ell_1,\dots,\ell_r}) \geq \binom{n}{r}\frac{F(G, \mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r})}{n}.$$

Para demostrar la proposición 2.2 usamos conjuntos $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-libres en grupos abelianos finitos para construir hipergrafos $K^{(r)}_{\ell_1,\dots,\ell_r}$-libres. La proposición 2.2

conecta resultados de problemas extremales en grupos abelianos con resultados de problemas extremales en hipergrafos. Recordamos a continuación un caso particular bien conocido.

Si A es un conjunto de Sidon en un grupo abeliano finito G, entonces el grafo $\mathcal{G}(V, \mathcal{E})$, donde $V = G$ y $\mathcal{E} = \{\{x, y\} : \ x + y \in A\}$, no contiene al grafo bipartito $K_{2,2}$. De no ser así tendríamos cuatro vértices dispuestos del modo siguiente:

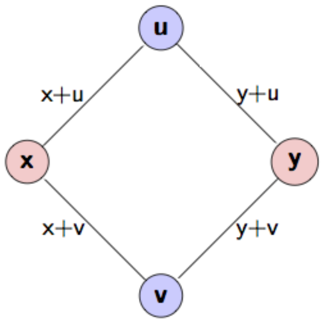

Figura 6: Grafo bipartito $K_{2,2}$.

Esto implicaría que $\{x, y\} + \{u, v\} \subset A$, contradiciendo la hipótesis de que A es $\mathcal{L}_{2,2}$-libre. A partir de esta observación y contando el número de aristas obtenemos

$$\mathrm{ex}(n, K_{2,2}) \geq |\mathcal{E}| \geq \binom{n}{2} \frac{F(G, \mathcal{L}_{2,2})}{n}, \qquad (n = |G|).$$

Conexión con problemas extremales en matrices

Los problemas extremales en conjuntos $\mathcal{L}$-libres también se pueden relacionar con problemas extremales en matrices.

Sea $A = (a_{i_1,\ldots,i_d})$ una matriz d-dimensional $n_1 \times \cdots \times n_d$, con $1 \leq i_\ell \leq n_\ell$ $(1 \leq \ell \leq d)$. Decimos que A es una matriz cero-uno cuando todas sus entradas son o bien 0 o bien 1.

Diremos que una matriz d-dimensional cero-uno A *contiene* a otra matriz cero-uno P si A tiene una sub-matriz que puede transformarse en P cambiando cualquier cantidad de unos a ceros. En otro caso, diremos que A *evita* a P.

Definición 2.5 *Sean d y n enteros positivos cualesquiera, y P una matriz d-dimensional. Llamaremos $f(n, P, d)$ al número máximo de unos en una matriz cero-uno d-dimensional $n \times \cdots \times n$ que evite a P.*

Nótese que una matriz cero-uno d-dimensional $n_1 \times \cdots \times n_d$ puede ser identificada con un hipergrafo d-uniforme (y viceversa). En la siguiente definición capturamos esta identificación.

Definición 2.6

1. *Sea A una matriz cero-uno d-dimensional $n_1 \times \cdots \times n_d$. Llamaremos $\mathcal{G}(A) := (V, \mathcal{E})$ al hiper-grafo de $n_1 + \cdots + n_d$ vértices $V = \bigcup_{1 \le \ell \le d} V_\ell$, con $V_\ell = \{1, 2, \ldots, n_\ell\}$, tal que $\{i_1, \ldots, i_d\} \in \mathcal{E}$ si y sólo si $a_{i_1,\ldots,i_d} = 1$*
2. *Sea $G = (V, \mathcal{E})$ un hipergrafo d-uniforme con $V = \bigcup_{1 \le \ell \le d} V_\ell$, y $|V_\ell| = n_\ell$. Llamemos $\mathcal{M}(G) := A$ a la matriz cero-uno d-dimensional $n_1 \times \cdots \times n_d$, tal que $a_{i_1,\ldots,i_d} = 1$ si y sólo si $\{i_1, \ldots, i_\ell\} \in \mathcal{E}$.*

Por definición $\mathcal{G}(A)$ tiene tantas hiperaristas como unos tiene la matriz A.

Esta identificación trae como consecuencia inmediata una primera conexión entre problemas extremales en hipergrafos y problemas extremales en matrices.

Proposición 2.3 *Sean d y n enteros positivos cualesquiera, y P una matriz d-dimensional cero-uno. Tenemos*

$$f(n, P, d) = ex(dn, \mathcal{G}(P)).$$

Llamaremos $R^{k_1,\ldots,k_d}$ a la matriz d-dimensional $k_1 \times \cdots \times k_d$ con uno en todas sus entradas. Estimar $f(n, R^{k_1,k_2}, 2)$ se conoce como el problema de Zarankiewicz. Es fácil comprobar que el grafo correspondiente a R^{k_1,k_2} es el completo bipartito K_{k_1,k_2}.

En el caso general, Geneson y Tian [25, teorema 2.2] demostraron que

$$f(n, R^{k_1,\ldots,k_d}, d) = O(n^{d-\alpha(k_1,\ldots,k_d)}), \qquad \text{donde } \alpha = \frac{\text{máx}(k_1, \ldots, k_d)}{k_1 k_2 \cdots k_d}. \tag{0.6}$$

Nosotros refinamos la estimación (0.6) utilizando el teorema 2.6 y la proposición 2.3.

Corolario 2.1 *Para cualesquiera* $2 \leq k_1 \leq k_2 \leq \cdots \leq k_d$*, tenemos*

$$f(n, R^{k_1,\dots,k_d}, d) \leq \frac{(k_d-1)^{\alpha} d^{d-\alpha}}{d!} n^{d-\alpha}(1+o(1)), \quad \textit{donde } \alpha = \frac{1}{k_1 k_2 \cdots k_{d-1}}.$$

Sucesiones infinitas $\mathcal{L}$-libres densas

El problema de encontrar sucesiones infinitas $\mathcal{L}$-libres con densidad extremal parece más difícil que el problema análogo para el caso finito.

En vista de la conjetura 2.1 para el caso finito, podríamos ser optimistas y creer que existe una sucesión $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-libre tal que $A(x) \gg x^{1-1/(\ell_1\cdots\ell_{r-1})}$. Erdős demostró que esto es imposible para las sucesiones $\mathcal{L}_{2,2}$-libres (sucesiones de Sidon). Nosotros generalizamos este hecho del modo siguiente.

Teorema 2.7 *Sean* $r \geq 2$ *y* $2 \leq \ell_1 \leq \cdots \leq \ell_r$ *enteros. Si* A *es una sucesión infinita* $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$*-libre, entonces tenemos*

$$\liminf_{x\to\infty} \frac{A(x)}{x} (x \log x)^{1/(\ell_1\cdots\ell_{r-1})} \ll 1.$$

Por tanto, una pregunta natural es si es cierto o no que para cualquier ϵ existe una sucesión infinita $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-libre tal que $A(x) \gg x^{1-1/(\ell_1\cdots\ell_{r-1})-\epsilon}$.

Erdős conjeturó que la respuesta a esta pregunta es positiva para el caso de sucesiones de Sidon. Ruzsa [42] y Cilleruelo [8] obtuvieron -utilizando construcciones distintas- las sucesiones de Sidon A más densas conocidas hasta la fecha, que satisfacen $A(x) \gg x^{\sqrt{2}-1+o(1)}$. La construcción de Ruzsa es probabilística mientras que la de Cilleruelo es explícita.

En vista del teorema 2.2, tiene sentido intentar adaptar la construcción probabilísitica del caso finito (véase §2.3.2) al caso infinito, para intentar demostrar que dado cualquier $\epsilon > 0$ existe una sucesión $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-libre tal que

$$A(x) \gg x^{1-\gamma-\epsilon}, \text{ con } \gamma = \frac{\ell_1+\cdots+\ell_r - r}{\ell_1\cdots\ell_r - 1}.$$

Aunque no hemos encontrado una prueba para el caso general, sí lo hemos conseguido en dos casos particulares relevantes.

Teorema 2.8 *Para cualesquiera $\ell \geq 2$ y $\epsilon > 0$ existe una sucesión infinita $\mathcal{L}_{2,\ell}$-libre con*

$$A(x) \gg x^{1-\frac{\ell}{2\ell-1}-\epsilon}.$$

Nótese que las construcciones en [42] y [8] proporcionan un exponente mayor para $\ell = 2$ y $\ell = 3$.

Teorema 2.9 *Para cualesquiera $r \geq 2$ y $\epsilon > 0$ existe una sucesión infinita $\mathcal{L}^{(r)}_{2,\dots,2}$-libre con*

$$A(x) \gg x^{1-\frac{r}{2^r-1}-\epsilon}.$$

Palíndromos en sucesiones de recurrencia linenl

Incluyo también en el último capítulo un resultado sobre un tema distinto al central de este trabajo, resultado que fue el primer paso en mi investigación de postgrado.

Es probable que $F_6 = 55$ sea el mayor número de Fibonacci que es también palíndromo. Sin embargo, parece un problema difícil decidir si solamente hay una cantidad finita de este tipo de números. Luca demostró que para cualquier base $b \geq 2$, el conjunto $\{n\colon F_n$ es palíndromo en base $b > 1\}$ tiene densidad cero [35]. Utilizamos una aproximación diferente para demostrar un resultado más general para una clase más amplia de sucesiones lineales recurrentes.

Teorema 3.1 *Sea $b \geq 2$ un entero y sea $\{a_n\}_{n\geq 1}$ una sucesión recurrente lineal de enteros con relación minimal de congruencia*

$$a_{n+k} = c_1 a_{n+k-1} + \cdots + c_k a_n, \qquad (n \geq 1),$$

donde $c_i \in \mathbb{Z}$ *para* $1 \leq i \leq k$. *Si el polinomio* $C(X) = X^k - c_1X^{k-1} - \cdots - c_k$ *tiene una única raíz dominante* $\alpha_1 > 0$ *que es multiplicativamente independiente de* b, *entonces existe* $c = c(b) > 0$ *tal que*

$$\#\{n \leq x\colon\ a_n \text{ es palíndromo en base } b\} = O(x^{1-c}).$$

Un corolario inmediato es que la cantidad de números de Fibonacci que son palíndromos en cualquier base es $O(x^{1-c})$, para cierta constante $c > 0$. Demostramos que en este caso podemos tomar $c = 10^{-11}$.

Corollario 3.1 *Sea* $\{F_n\}$ *la sucesión de Fibonacci. Tenemos*

$$\#\{n \leq x\colon\ F_n \text{ es palíndromo en base } 10\} \ll x^{1-10^{-11}}.$$

Los resultados incluidos en este trabajo aparecieron originalmente en los siguientes artículos de investigación:

[13] Cilleruelo, Javier; Tesoro, Rafael. Dense infinite B_h sequences. *Publ. Mat.* 59 (2015), no. 1, 55–73.

[14] Cilleruelo, Javier; Tesoro, Rafael. On sets free of sumsets with summands of prescribed size. *Combinatorica* (aceptado en 2015 para publicación)

[15] Cilleruelo, Javier; Tesoro, Rafael; Luca, Florian. Palindromes in linear recurrence sequences. *Monatsh. Math.* 171 (2013), no. 3-4, 433–442.

[40] Peng, Xing; Tesoro, Rafael; Timmons, Craig. Bounds for generalized Sidon sets. *Discrete Math.* 338 (2015), no. 3, 183–190.

Summary and conclusions

The present work is focused in the study of finite sets and infinite sequences of positive integers with certain arithmetic restrictions of additive kind. In chapter 1 we study sequences of integers where all the sums of h elements of the sequence are distinct. These sequences are called B_h sequences. In chapter 2 we study sequences of integers that do not contain sumsets $L_1+\cdots+L_r$ where the sizes of the summands are fixed, $|L_i| = \ell_i,\ i = 1,\ldots,r$. We will call these sequences $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free sequences, and in a generic way $\mathcal{L}$-free sequences. We also study finite $\mathcal{L}$-free sets within intervals of integers and within finite abelian groups.

B_h sequences and $\mathcal{L}$-free sequences are two natural generalizations of the Sidon sequences, introduced by Erdős. Sidon sequences are those sequences of integers such that all the non-null differences of two of their elements are distinct. Both B_2 sequences as well as $\mathcal{L}_{2,2}$-free sequences are precisely Sidon sequences.

Although it is easy to construct sequences with this kind of restrictions, the challenge is to construct them with the largest possible density. It is natural to think that the denser a sequence is the more difficult is that such a sequence satisfies a restriction of the ones above mentioned. To construct dense sequences with the aforementioned restrictions and to attain upper bounds for these densities are the central objectives of this work. We also study the analogous problems for the case of finite $\mathcal{L}$-free sets.

Other sequences with different additive restrictions have been studied in the literature, the more popular being the sequences that avoid arithmetic progressions of length k. Szemerédi's Theorem, central in this area, claims that such sequences have density 0 for all $k \geq 3$.

A last chapter is devoted to palindromic numbers in the Fibonacci series, which has nothing to do with the main topic of this thesis, but which was part of my work during my period as Ph.D. student.

Dense B_h sequences

Let $h \geq 2$ be an integer. We say that a sequence $\mathcal{B}$ of positive integers is a B_h sequence if all the sums

$$b_1 + \cdots + b_h, \qquad (b_k \in \mathcal{B},\ 1 \leq k \leq h),$$

are distinct subject to $b_1 \leq b_2 \leq \cdots \leq b_h$. The same definition can be used for B_h finite sets.

B_2 sets and B_2 sequences are usually known as Sidon sets and Sidon sequences respectively. In this particular case, the arithmetic restriction of all sums $b_1 + b_2,\ (b_k \in \mathcal{B},\ b_1 \leq b_2)$, being distinct is equivalent to require that the $\mathcal{B}$ sequence does not have four elements arranged as shown below:

Figure 7: Forbidden arrangement in Sidon sequences/sets.

The reason is that if a sequence contains four elements as in the figure 7, then it would contain two distinct pairs of elements $\{b_1, b_1'\}, \{b_2', b_2\}$ such that $b_1' - b_1 = b_2 - b_2'$, that is to say $b_1 + b_2 = b_1' + b_2'$, with $\{b_1, b_2\} \neq \{b_1', b_2'\}$. Hence B_2 sequences are characterized by avoiding the arrangement in figure 7.

Given any infinite sequence of integers A, we define its *counting function* as $A(x) = \{a \in A \colon a \leq x\}$. The study of the counting function of infinite B_h sequences (or the size of finite B_h sets) is a classic topic in combinatorial number theory. A simple counting argument proves that if $\mathcal{B} \subset [1, n]$ is a B_h set then $|\mathcal{B}| \leq (C_h + o(1))n^{1/h}$ for a constant C_h (see [9] and [26] for non trivial upper bounds for C_h) and consequently that $\mathcal{B}(x) \ll x^{1/h}$ when $\mathcal{B}$ is an infinite B_h sequence.

Erdős conjectured the existence, for all $\epsilon > 0$, of an infinite B_h sequence $\mathcal{B}$ with counting function $\mathcal{B}(x) \gg x^{1/h-\epsilon}$. It is believed that ϵ cannot be removed from the last exponent, a fact that has only been proved for h even. The *greedy* algorithm produces an infinite B_h sequence $\mathcal{B}$ with

$$\mathcal{B}(x) \gg x^{\frac{1}{2h-1}} \quad (h \geq 2). \tag{0.7}$$

For the case $h = 2$, Atjai, Komlós and Szemerédi [1] proved that there exists a B_2 sequence with $\mathcal{B}(x) \gg (x \log x)^{1/3}$, improving by a power of a logarithm the lower bound (0.7). The largest improvement of (0.7) for the case $h = 2$ was achieved by Ruzsa [?]. He constructed, in a clever way, an infinite Sidon sequence $\mathcal{B}$ satisfying

$$\mathcal{B}(x) = x^{\sqrt{2}-1+o(1)}. \tag{0.8}$$

In chapter 1 we adapt Ruzsa's ideas to construct dense infinite B_3 and B_4 sequences, and in this way we improve, for the first time, the lower bound (0.7) for $h = 3$ and $h = 4$.

Theorem 1.1 *For $h = 2, 3, 4$ there is an infinite B_h sequence $\mathcal{B}$ with counting function*

$$\mathcal{B}(x) = x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}.$$

After our work on this subject [13], Cilleruelo [8] obtained the same growing function (0.8) for dense infinite Sidon sequences using a different construction than Ruzsa's. In addition, Cilleruelo adapted his construction to prove Theorem 1.1 for all $h \geq 2$.

$\mathcal{L}$-free sets and sequences

B_h sets and sequences are one possible generalization of Sidon sets and sequences. In chapter 2 we study extremal problems in the context of another natural generalization of Sidon sets and sequences. We also show the connections of such problems with extremal problems on graphs and hyper-graphs and with certain extremal problems on matrices.

The core definition for all the second part of this work is the following concept, to which we will refer with the generic expression *"$\mathcal{L}$-free"* :

Definition 2.1 *Let $r, \ell_1, \dots, \ell_r$ be integers with $r \geq 1$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$. Given an abelian group G we say that $A \subset G$ is a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set if A does not contain any sumset of the form*

$$L_1 + \cdots + L_r = \{\lambda_1 + \cdots + \lambda_r : \ \lambda_i \in L_i, \ i = 1, \dots, r\},$$

with $|L_i| = \ell_i, \ i = 1, \dots, r$. For $r = 2$ we simply write $\mathcal{L}_{\ell_1,\ell_2}$.

As usual in the mathematical literature we call *sumset* to $L_1 + \cdots + L_r$.

In chapter 2 we study $\mathcal{L}$-free finite sets and $\mathcal{L}$-free infinite sequences, that is to say, with the restriction of being free of sumsets with summands of prescribed size.

To motivate Definition 2.1 we recall several particular cases of this arithmetic restriction, that have already being studied in the literature.

1. *$\mathcal{L}_{2,2}$-free sets.* We can represent a sumset $L_1 + L_2$ with summands of 2 elements as two copies of a pair of points:

   

   Each point represents a sum in L_1+L_2. This is the same arrangement as the one in figure 7. It is clear that any set containing this arrangement of four points would have two distinct pairs of elements with the same distance within each pair. In other words: the Sidon sets are precisely the $\mathcal{L}_{2,2}$-free sets.

2. *$\mathcal{L}_{2,\ell}$-free sets.* A $\mathcal{L}_{2,\ell}$-free set A is characterized by the property that there are no more than $\ell - 1$ different ways to express any non-zero element in the ambient group as a difference of two elements of A. They have been called $B_2^{\circ}[\ell - 1]$ sets [32] and $B_2^{-}[\ell - 1]$ sets [45].

   For example the typical shape of a sumset $L_1 + L_2$ with $|L_1| = 2$ and $|L_2| = 3$ is two copies of one pair of points:

Figure 8: Forbidden arrangement in $\mathcal{L}_{2,3}$-free sets/sequences.

The $\mathcal{L}_{2,3}$-free sets are characterized as being free of arrangements of six elements as the one in figure 8.

3. $\mathcal{L}_{\ell_1,\ell_2}$*-free sets.* The sets that do not contain ℓ_2 copies of sets with ℓ_1 elements were introduced by Erdős and Harzheim [18] and have been further studied in [40]. For example the $\mathcal{L}_{3,4}$-free sets are characterized by avoiding four copies of three points, an arrangement that we can represent as follows:

Figure 9: Forbidden arrangement in $\mathcal{L}_{3,4}$-free sets/sequences.

4. $\mathcal{L}^{(r)}_{2,\dots,2}$*-free sets* A Hilbert cube of dimension r is a sumset of the form $L_1+\cdots+L_r$ with $|L_1|=\cdots=|L_r|=2$. Thus $\mathcal{L}^{(r)}_{2,\dots,2}$-free sets are those free of Hilbert cubes of dimension r. A Hilbert cube of dimension 3 has this shape:

Figure 10: 3-dimensional Hilbert cube, forbidden in $\mathcal{L}_{2,2,2}$-free sets.

Firstly a pair of points is copied twice, in the left part of the figure 10 (this part is the same as the figure 7). Afterwards this left part is copied at the right side of the page and we finally obtain the 8 points of a Hilbert cube of dimension 3.

Note that some of the sums in $L_1+\cdots+L_r$ might be repeated and in these cases (that we will call degenerate) the representations of sums would have less points that the ones we have drawn. For example: the sumset $\{2,3\}+\{1,2\}=\{3,4,5\}$ has three elements, instead of four, and can be represented as follows:

Figure 11: Another forbidden arrangement in Sidon sets/sequences

In other words: any sequence that contains $\{3,4,5\}$ is not a Sidon sequence and although it may avoid the arrangement in figure 7, it cannot avoid the arrangement in figure 11.

Extremal $\mathcal{L}$-free finite sets

We discuss extremal finite $\mathcal{L}$-free sets within the interval $\{1,\dots,n\}$ in §2.1.1 and in §2.3. Our main results can be summarized as follows.

Let $F\big(n,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}\big)$ denote the size of a largest $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set in the interval $\{1,\dots,n\}$. The general upper bound that we attain recovers known upper bounds for the particular cases that we have reminded in the previous pages.

Theorem 2.1 *For any $r\geq 2$ and $2\leq \ell_1\leq\cdots\leq\ell_r$ we have*

$$F\big(n,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}\big)\leq(\ell_r-1)^{\frac{1}{\ell_1\cdots\ell_{r-1}}}n^{1-\frac{1}{\ell_1\cdots\ell_{r-1}}}+O\left(n^{\frac{1}{2}+\frac{1}{2\ell_{r-1}}-\frac{1}{\ell_1\cdots\ell_{r-1}}}\right).$$

Let us compare Theorem 2.1 with the know upper bounds for the aforementioned particular cases:

i) $\mathcal{L}_{2,2}$*-free sets.* The upper bound $|A|\leq\sqrt{n}+O(n^{1/4})$ for any Sidon set $A\subset\{1,\dots,n\}$ was proved by Erdős and Turán [22] and refined until $|A|<\sqrt{n}+n^{1/4}+1/2$ by other authors [33, 41, 10]. The Erdős-Turán bound follows from Theorem 2.1 for $r=\ell_1=\ell_2=2$.

ii) $\mathcal{L}_{2,\ell}$*-free sets.* The upper bound $|A|<\sqrt{(\ell-1)n}+((\ell-1)n)^{1/4}+1/2$ for $B_2^{\circ}[\ell-1]$ sets $A\subset\{1,\dots,n\}$ was proved in [10]. Theorem 2.1 for $r=\ell_1=2$ and $\ell_2=\ell\geq 2$ gives

$$F(n,\mathcal{L}_{2,\ell})\leq(\ell-1)^{1/2}n^{1/2}+O(n^{\frac{1}{4}}).$$

iii) $\mathcal{L}_{\ell_1,\ell_2}$*-free sets.* Peng, Tesoro and Timmons [40] proved that if $A\subset\{1,\dots,n\}$ does not contain ℓ_1 copies of any set of ℓ_2 elements then $|A|\leq$

$(\ell_2-1)^{1/\ell_1}n^{1-1/\ell_1}+O\left(n^{1/2-1/(2\ell_1)}\right)$. This also follows from Theorem 2.1 for $r=2$. Note that Erdős and Harzheim [18] had previously proved the weaker estimate $|A|\ll n^{1-1/\ell_1}$ for these sets.

iv) $\mathcal{L}^{(r)}_{2,\dots,2}$-*free sets.* Csaba Sándor [43] proved that if $A\subset\{1,\dots,n\}$ does not contain a Hilbert cube of dimension r then $|A|\le n^{1-1/2^{r-1}}+2n^{1-1/2^{r-2}}$, except for finitely many n. Theorem 2.1 in the case $\mathcal{L}^{(r)}_{2,\dots,2}$ implies
$$F(n,\mathcal{L}^{(r)}_{2,\dots,2})\le n^{1-1/2^{r-1}}+O\left(n^{3/4-1/2^{r-1}}\right),$$
which improves the error term for $r\ge 4$ in Sándor's estimate.

In the other direction, using the probabilistic method, we obtain a lower bound for the general case.

Theorem 2.2 *For any $r\ge 2$ and $2\le\ell_1\le\cdots\le\ell_r$ we have*
$$F(n,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r})\ge n^{1-\frac{\ell_1+\cdots+\ell_r\ -r}{\ell_1\cdots\ell_r\ -1}-o(1)}.$$

The exponents in these lower and upper bounds are distinct and to close the gap between them is a major problem. We think that the exponent for $\mathcal{L}$-free extremal sets in intervals is the one attained in the upper bound:

Conjecture 2.1 *For any $r\ge 2$ and $2\le\ell_1\le\cdots\le\ell_r$, we have*
$$F(n,\mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r})\asymp n^{1-1/(\ell_1\cdots\ell_{r-1})}.$$

This conjecture is known true for the particular case
$$F(n,\mathcal{L}_{2,\ell_2})\sim(\ell_2-1)^{1/2}n^{1-1/2}.$$

This last asymptotic in the particular case $\ell_2=2$ recovers the estimate found by Erdős and Turán [22] for extremal Sidon sets and was generalized to any $\ell_2\ge 2$ by Trujillo-Solarte, García-Pulgarín and Velásquez-Soto [45]. We have proved Conjecture 2.1 true in two additional cases:
$$F(n,\mathcal{L}_{3,\ell_2})\asymp n^{1-1/3},\quad(\ell_2\ge 3),$$
$$F(n,\mathcal{L}_{\ell_1,\ell_2})\asymp n^{1-1/\ell_1},\quad(\ell_2\ge \ell_1!+1).$$

These two cases are immediate consequences of Theorem 2.3 and of Theorem 2.4 resp.

Theorem 2.3 *For any integer $n \geq 1$, there is a $\mathcal{L}_{3,3}$-free set $A \subset \{1,\dots,n\}$ with*

$$|A| \geq \left(4^{-2/3}+o(1)\right) n^{2/3}.$$

Theorem 2.4 *Let $\ell \geq 2$ be an integer. For any integer $n \geq 1$, there is a $\mathcal{L}_{\ell,\ell!+1}$-free set $A \subset [n]$ with*

$$|A| = (1+o(1))\left(\frac{n}{2^{\ell-1}}\right)^{1-1/\ell}.$$

In §2.1.1 we also study extremal finite $\mathcal{L}$-free sets living in a finite abelian group G. We will denote by $F(G,\mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r})$ the largest size of a $\mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r}$-free set in G.

We obtain the following lower bound for subsets of $\mathbb{Z}^3_{p-1}$ that are free of Hilbert cubes of dimension 3:

Theorem 2.5 *For any prime $p \geq 2$ we have*

$$F(\mathbb{Z}^3_{p-1},\mathcal{L}^{(3)}_{2,2,2}) \geq (p-3)^2.$$

As a consequence of Theorem 2.5 we confirm, with a different construction, the lower bound

$$F(n,\mathcal{L}^{(3)}_{2,2,2}) \gg n^{1-1/3},$$

that was attained by Katz, Krop and Maggioni [29]. This estimate improves the lower bound $F(n,\mathcal{L}^{(3)}_{2,2,2}) \gg n^{1-3/7-o(1)}$ given by Theorem 2.2.

The extremal size in intervals and the extremal size in finite groups are related as follows:

Proposition 2.1 *For any $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ and $n_1,\cdots,n_k$, we have*

$$F(2^{k-1}n_1\cdots n_k,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}) \geq F(\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k},\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}).$$

Connections with extremal graph problems

Given a graph (or hypergraph) $\mathcal{H}$, let $\mathrm{ex}(n, \mathcal{H})$ denote the maximum number of edges (or hyperedges) of a n vertices graph (or hypergraph) which does not contain $\mathcal{H}$ as a sub-graph (or sub-hypergraph). Estimating $\mathrm{ex}(n, \mathcal{H})$ is a major problem in extremal graph theory.

In §2.1.2, §2.1.3, §2.4.1 and §2.4.2 we present and we prove connections between $\mathcal{L}$-free problems and the Turán problem in graphs and hyper-graphs. In order to summarize these connections, we first define the r-uniform hypergraph.

Definition 2.4 *Let $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ be integers. We write $K^{(r)}_{\ell_1,\dots,\ell_r}$ for the r-uniform hypergraph $(V, \mathcal{E})$ where $V = V_1 \cup \cdots \cup V_r$ with $|V_i| = \ell_i,\ i = 1, \dots, r$ and*

$$\mathcal{E} = \{\{x_1, \dots, x_r\} :\ x_i \in V_i,\ i = 1, \dots, r\}.$$

We will say that the r-hypergraph $\mathcal{G}$ is $K^{(r)}_{\ell_1,\dots,\ell_r}$-free when $\mathcal{G}$ does not contain any r-uniform hypergraph $K^{(r)}_{\ell_1,\dots,\ell_r}$

An easy probabilistic argument gives the following lower bound

$$n^{r-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}} \ll \mathrm{ex}(n; K^{(r)}_{\ell_1,\cdots,\ell_r}). \tag{0.9}$$

The upper bound was considered by Erdős in the case $\ell = \ell_1 = \cdots = \ell_r$. He proved [17, Theorem 1] that

$$ex(n, K^{(r)}_{\ell,\dots,\ell}) \ll n^{r-1/\ell^{r-1}}. \tag{0.10}$$

We have refined and generalized the estimate (0.10) as follows.

Theorem 2.6 *For all $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$, we have*

$$ex(n, K^{(r)}_{\ell_1,\dots,\ell_r}) \leq \frac{(\ell_r - 1)^{1/\ell_1\cdots\ell_{r-1}}}{r!}\, n^{r-1/\ell_1\cdots\ell_{r-1}}(1 + o(1)), \quad (n \to \infty). \tag{0.11}$$

The case $r = 2$ in Theorem 2.6 was proved by Kövari, Sós and Turán [31]. It is believed that the upper bound in (0.11) is not far from the real value of $ex(n, K^{(r)}_{\ell_1,\dots,\ell_r})$.

Conjecture 2.2

$$ex(n, K^{(r)}_{\ell_1,\cdots,\ell_r}) \asymp n^{r-1/\ell_1\cdots\ell_{r-1}}.$$

The two exponents of n in Theorems 2.1 and 2.2 have the same flavour as the two exponents of n in (0.9) and in (0.11) Theorem 2.6. The following result explains this resemblance.

Proposition 2.2 *Let G be a finite abelian group with $|G| = n$. Then*

$$ex(n, K^{(r)}_{\ell_1,\ldots,\ell_r}) \geq \binom{n}{r} \frac{F(G, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r})}{n}.$$

To proof this we use $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free sets in finite abelian groups to construct $K^{(r)}_{\ell_1,\ldots,\ell_r}$-free hypergraphs. Proposition 2.2 connects results on extremal problems in abelian groups with results on extremal problems in hypergraphs. We recall next one well known particular case.

If A is a Sidon set in a finite abelian group G then the graph $\mathcal{G}(V, \mathcal{E})$ where $V = G$ and $\mathcal{E} = \{\{x, y\} : \ x + y \in A\}$ does not contain the bipartite $K_{2,2}$. Otherwise, we would have four vertices arranged as follows:

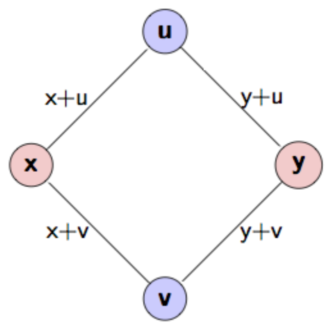

Figure 12: Bipartite graph $K_{2,2}$.

This would imply that $\{x, y\} + \{u, v\} \subset A$, contradicting the assumption that A is $\mathcal{L}_{2,2}$ -free. Parting from this observation and counting the number of edges we get

$$\mathrm{ex}(n, K_{2,2}) \geq |\mathcal{E}| \geq \binom{n}{2} \frac{F(G, \mathcal{L}_{2,2})}{n}, \qquad (n = |G|).$$

Connection with extremal problems on matrices

$\mathcal{L}$-free extremal problems can also be related with extremal problems in matrices.

Let $A = (a_{i_1,\ldots,i_d})$ be a d-dimensional $n_1 \times \cdots \times n_d$ matrix, with $1 \leq i_\ell \leq n_\ell$ $(1 \leq \ell \leq d)$. We will say that A is a zero-one matrix if all its entries are either 0 or 1.

We will say that a d-dimensional zero-one matrix A *contains* another zero-one matrix P if A has a sub-matrix that can be transformed into P by changing any number of ones to zeros. Otherwise, we will say that A *avoids* P.

Definition 2.5 *Let d and n be any positive integers, and let P be a given d-dimensional matrix. We will call $f(n, P, d)$ to the maximum number of ones in a d-dimensional $n \times \cdots \times n$ zero-one matrix that avoids P.*

Note that a d-dimensional $n_1 \times \cdots \times n_d$ zero-one matrix can be identified with a d-uniform hyper-graph (and vice versa). In the following definition we capture this identification.

Definition 2.6

1. *Let A be a given d-dimensional $n_1 \times \cdots \times n_d$ zero-one matrix. Let us denote by $\mathcal{G}(A) := (V, \mathcal{E})$ the hyper-graph of $n_1 + \cdots + n_d$ vertices $V = \bigcup_{1 \leq \ell \leq d} V_\ell$, with $V_\ell = \{1, 2, \ldots, n_\ell\}$ and hyper-edges $\mathcal{E} = \{\{i_1, \ldots, i_d\} : a_{i_1,\ldots,i_d} = 1\}$.*

2. *Let $G = (V, \mathcal{E})$ be a d-uniform hyper-graph with $V = \bigcup_{1 \leq \ell \leq d} V_\ell$, with $|V_\ell| = n_\ell$. Let us denote by $\mathcal{M}(G)$ the d-dimensional $n_1 \times \cdots \times n_d$ zero-one matrix with $a_{i_1,\ldots,i_d} = 1$ if and only if $\{i_1, \ldots, i_\ell\} \in \mathcal{E}$, where $A = \mathcal{M}(G)$.*

By definition $\mathcal{G}(A)$ has as many hyper-edges as ones has the matrix A.

This identification immediately brings a first connection between extremal problems in hypergraphs and extremal problems in matrices.

Proposition 2.3 *Let d and n be any positive integers, and let P be a* *given zero-one d-dimensional matrix. Then we have*

$$f(n,P,d) = ex\,(dn, \mathcal{G}(P)). \tag{0.12}$$

Let $R^{k_1,\dots,k_d}$ denote the d-dimensional $k_1 \times \cdots \times k_d$ matrix of all ones. Estimating $f(n, R^{k_1,k_2}, 2)$ is known as the Zarankiewicz problem. It is easy to check that the graph corresponding to R^{k_1,k_2} is the complete bipartite K_{k_1,k_2}.

In the general case Geneson and Tian [25, Theorem 2.2] proved that

$$f(n, R^{k_1,\dots,k_d}, d) = O(n^{d-\alpha(k_1,\dots,k_d)}), \qquad \text{where } \alpha = \frac{\max(k_1,\dots,k_d)}{k_1 k_2 \cdots k_d}. \tag{0.13}$$

We refine the estimate (0.13) using Theorem 2.6 and Proposition 2.3.

Corollary 2.1 *Let $2 \le k_1 \le k_2 \le \cdots \le k_d$. Then we have*

$$f(n, R^{k_1,\dots,k_d}, d) \le \frac{(k_d-1)^\alpha d^{d-\alpha}}{d!}\, n^{d-\alpha}(1+o(1)), \quad \text{where } \alpha = \frac{1}{k_1 k_2 \cdots k_{d-1}}.$$

Dense $\mathcal{L}$-free infinite sequences

The problem of finding $\mathcal{L}$-free infinite sequences with extremal density seems more difficult that the analogous problem for the finite case.

In view of Conjecture 2.1 for the finite case, we might be optimistic believing in the existence of a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sequence A such that $A(x) \gg x^{1-1/(\ell_1\cdots\ell_{r-1})}$. Erdős proved this impossible for the $\mathcal{L}_{2,2}$-free sequences (Sidon sequences). We generalize this fact as follows.

Theorem 2.7 *If A is a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sequence then we have*

$$\liminf_{x\to\infty} \frac{A(x)}{x}(x\log x)^{1/(\ell_1\cdots\ell_{r-1})} \ll 1.$$

Hence a natural question is whether or not it is true that for any ϵ there exists a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free infinite sequence with $A(x) \gg x^{1-1/(\ell_1\cdots\ell_{r-1})-\epsilon}$.

Erdős conjectured a positive answer to this question for the case of Sidon sequences. Ruzsa [42] and Cilleruelo [8] attained -using different constructions- the densest Sidon sequences known up to date, that satisfy $A(x) \gg x^{\sqrt{2}-1+o(1)}$. Ruzsa's construction is probabilistic whereas Cilleruelo's construction is explicit.

In view of Theorem 2.2, it does make sense to try to adapt the probabilistic construction of the finite case (see §2.3.2), aiming to prove that for any $\epsilon > 0$ there exists a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sequence such that

$$A(x) \gg x^{1-\gamma-\epsilon}, \text{ with } \gamma = \frac{\ell_1 + \cdots + \ell_r - r}{\ell_1 \cdots \ell_r - 1}.$$

Although we have not found a proof for the general case, we did succeed in two particular relevant cases.

Theorem 2.8 *For any* $\ell \geq 2$ *and for any* $\epsilon > 0$ *there exists an infinite* $\mathcal{L}_{2,\ell}$*-free sequence with*

$$A(x) \gg x^{1-\frac{\ell}{2\ell-1}-\epsilon}.$$

Note however that the constructions in [42] and [8] provide a greater exponent for $\ell = 2$ and $\ell = 3$.

Theorem 2.9 *For any* $r \geq 2$ *and for any* $\epsilon > 0$ *there exists an infinite* $\mathcal{L}^{(r)}_{2,\dots,2}$*-free sequence with*

$$A(x) \gg x^{1-\frac{r}{2^r-1}-\epsilon}.$$

Palindromes in linear recurrence sequences

I also include in the last chapter a result on a topic distinct from the central topic of this work, result that was the first step in my postgraduate research.

Probably $F_6 = 55$ is the largest palindromic Fibonacci number. It seems, however, a hard problem to decide if there are only finitely many of these numbers. Luca proved that for any base $b \geq 2$, the set

$$\{n\colon F_n \text{ is palindromic in base } b > 1\}$$

has zero density [35]. We use a different approach to prove a stronger and more general result for a broader class of linear recurrence sequences.

Theorem 3.1 *Let $b \geq 2$ be an integer and let $\{a_n\}_{n\geq 1}$ be the linear recurrence sequence of integers of minimal recurrence relation*

$$a_{n+k} = c_1 a_{n+k-1} + \cdots + c_k a_n, \qquad (n \geq 1), \tag{0.14}$$

where $c_i \in \mathbb{Z}$ for $1 \leq i \leq k$. If the polynomial $C(X) = X^k - c_1 X^{k-1} - \cdots - c_k$ has a unique dominant root $\alpha_1 > 0$ which is multiplicatively independent with b, then there exists $c = c(b) > 0$ such that

$$\#\{n \leq x\colon\ a_n \textit{ is palindromic in base } b\} = O(x^{1-c}).$$

An immediate corollary is that the number of Fibonacci numbers up to x which are palindromes in any base is $O(x^{1-c})$, for some constant $c > 0$. We prove that in this case we can take $c = 10^{-11}$.

Corollary 3.1 *We have that*

$$\#\{n \leq x\colon\ F_n \textit{ is palindrome in base } 10\} \ll x^{1-10^{-11}}.$$

The results included in this thesis originally appeared in the following research articles:

[13] Cilleruelo, Javier; Tesoro, Rafael. Dense infinite B_h sequences. *Publ. Mat.* 59 (2015), no. 1, 55–73.

[14] Cilleruelo, Javier; Tesoro, Rafael. On sets free of sumsets with summands of prescribed size. *Combinatorica* (accepted in 2015 for publication)

[15] Cilleruelo, Javier; Tesoro, Rafael; Luca, Florian. Palindromes in linear recurrence sequences. *Monatsh. Math.* 171 (2013), no. 3-4, 433–442.

[40] Peng, Xing; Tesoro, Rafael; Timmons, Craig. Bounds for generalized Sidon sets. *Discrete Math.* 338 (2015), no. 3, 183–190.

Chapter 1

Dense infinite B_h sequences

1.1. Introduction

Let $h \geq 2$ be an integer. We say that a sequence $\mathcal{B}$ of positive integers is a B_h sequence if all the sums

$$b_1 + \cdots + b_h, \qquad (b_k \in \mathcal{B},\ 1 \leq k \leq h),$$

are distinct subject to $b_1 \leq b_2 \leq \cdots \leq b_h$. The study of the size of finite B_h sets or of the growing function of infinite B_h sequences are a classic topic in combinatorial number theory. A simple counting argument proves that if $\mathcal{B} \subset [1, n]$ is a B_h set then $|\mathcal{B}| \leq (C_h + o(1))n^{1/h}$ for a constant C_h (see [9] and [26] for non trivial upper bounds for C_h) and consequently that $\mathcal{B}(x) \ll x^{1/h}$ when $\mathcal{B}$ is an infinite B_h sequence.

Erdős conjectured the existence, for all $\epsilon > 0$, of an infinite B_h sequence $\mathcal{B}$ with counting function $\mathcal{B}(x) \gg x^{1/h-\epsilon}$. It is believed that ϵ cannot be removed from the last exponent, a fact that has only been proved for h even. On the other hand, the *greedy* algorithm produces an infinite B_h sequence $\mathcal{B}$ with

$$\mathcal{B}(x) \gg x^{\frac{1}{2h-1}} \quad (h \geq 2). \tag{1.1}$$

Up to now the exponent $1/(2h-1)$ is the largest known for the growth of a B_h sequence when $h \geq 3$. For further information about B_h sequences see [28, § II.2] or [39].

For the case $h = 2$, Atjai, Komlós and Szemerédi [1] proved that there exists a B_2 sequence (also called Sidon sequence) with $\mathcal{B}(x) \gg (x \log x)^{1/3}$, improving by a power of a logarithm the lower bound (1.1). So far the largest improvement of (1.1) for the case $h = 2$ was achieved by Ruzsa ([42]). He constructed, in a clever way, an infinite Sidon sequence $\mathcal{B}$ satisfying

$$\mathcal{B}(x) = x^{\sqrt{2}-1+o(1)}.$$

Our aim is to adapt Ruzsa's ideas to build dense infinite B_3 and B_4 sequences so to improve the lower bound (1.1) for $h = 3$ and $h = 4$.

Theorem 1.1. *For $h = 2, 3, 4$ there is an infinite B_h sequence $\mathcal{B}$ with counting function*

$$\mathcal{B}(x) = x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}.$$

The starting point in Ruzsa's construction were the numbers $\log p$, p prime, which form an infinite Sidon set of *real* numbers. Instead we start from the arguments of the Gaussian primes, which also have the same B_h property with the additional advantage of being a bounded sequence. This idea was suggested in [11] to simplify the original construction of Ruzsa and was written in detail for B_2 sequences in [37].

Since $\sqrt{(h-1)^2+1} - (h-1) \sim 1/(2(h-1))$ for $h \to \infty$ the construction is really meaningful for small values of h and perhaps not so for large ones.

1.2. The Gaussian arguments

For each rational prime $p \equiv 1 \pmod 4$ we consider the Gaussian prime $\mathfrak{p}$ of $\mathbb{Z}[i]$ such that

$$\mathfrak{p} := a + bi, \qquad p = a^2 + b^2, \quad a > b > 0,$$

so the argument $\theta(\mathfrak{p})$ of $\mathfrak{p} = \sqrt{p}\; e^{2\pi i\,\theta(\mathfrak{p})}$ is a real number in the interval $(0, 1/8)$. We will use several times throughout the paper the following lemma that can be seen as a measure of the quality of the B_h property of this sequence of real numbers.

Lemma 1.1. *Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_h, \mathfrak{p}'_1, \cdots, \mathfrak{p}'_h$ be distinct Gaussian primes satisfying $0 < \theta(\mathfrak{p}_r), \theta(\mathfrak{p}'_r) < 1/8,\ r = 1, \cdots, h$. The following inequality holds:*

$$\left| \sum_{r=1}^{h} (\theta(\mathfrak{p}_r) - \theta(\mathfrak{p}'_r)) \right| > \frac{1}{7\,|\mathfrak{p}_1 \cdots \mathfrak{p}_h\ \mathfrak{p}'_1 \cdots \mathfrak{p}'_h|}.$$

Proof. It is clear that

$$\sum_{r=1}^{h} (\theta(\mathfrak{p}_r) - \theta(\mathfrak{p}'_r)) \equiv \theta(\mathfrak{p}_1 \cdots \mathfrak{p}_h \overline{\mathfrak{p}'_1 \cdots \mathfrak{p}'_h}) \pmod 1. \tag{1.2}$$

Since $\mathbb{Z}[i]$ is a unique factorization domain, all the primes are in the first octant and they are all distinct, the Gaussian integer $\mathfrak{p}_1 \cdots \mathfrak{p}_h \overline{\mathfrak{p}'_1 \cdots \mathfrak{p}'_h}$ cannot be a real integer. Using this fact and the inequality $\arctan(1/x) > 0.99/x$ for $x \geq \sqrt{5 \cdot 13}$ (observe that 5 and 13 are the two smallest primes $p \equiv 1 \pmod 4$) we have

$$\begin{aligned} |\theta(\mathfrak{p}_1 \cdots \mathfrak{p}_h \overline{\mathfrak{p}'_1 \cdots \mathfrak{p}'_h})| &\geq \|\theta(\mathfrak{p}_1 \cdots \mathfrak{p}_h \overline{\mathfrak{p}'_1 \cdots \mathfrak{p}'_h})\| \\ &\geq \frac{1}{2\pi} \arctan\left(\frac{1}{|\mathfrak{p}_1 \cdots \mathfrak{p}_h \overline{\mathfrak{p}'_1} \cdots \overline{\mathfrak{p}'_h}|} \right) \\ &> \frac{1}{7|\mathfrak{p}_1 \cdots \mathfrak{p}_h \overline{\mathfrak{p}'_1} \cdots \overline{\mathfrak{p}'_h}|}, \end{aligned} \tag{1.3}$$

where $\| \cdot \|$ means the distance to $\mathbb{Z}$. The lemma follows from (1.2) and (1.3). □

We illustrate the B_h property of the arguments of the Gaussian primes with a quick construction of a finite B_h set which is only a $\log x$ factor below the optimal bound. Unfortunately this simple construction cannot be used for infinite B_h sequence because the elements of $\mathcal{A}$ depend on x.

Theorem 1.2. *The set*

$$\mathcal{A} = \left\{ \lfloor x\theta(\mathfrak{p}) \rfloor : \ |\mathfrak{p}| \leq \left(\frac{x}{7h} \right)^{\frac{1}{2h}} \right\} \subset [1, x]$$

is a B_h set with $|\mathcal{A}| \gg x^{1/h} / \log x$.

Proof. When

$$\lfloor x\theta(\mathfrak{p}_1)\rfloor + \cdots + \lfloor x\theta(\mathfrak{p}_h)\rfloor = \lfloor x\theta(\mathfrak{p}'_1)\rfloor + \cdots + \lfloor x\theta(\mathfrak{p}'_h)\rfloor$$

then

$$x\,|\theta(\mathfrak{p}_1) + \cdots + \theta(\mathfrak{p}_h) - \theta(\mathfrak{p}'_1) - \cdots - \theta(\mathfrak{p}'_h)| \le h.$$

If the Gaussian primes are distinct then Lemma 1.1 implies that

$$|\theta(\mathfrak{p}_1) + \cdots + \theta(\mathfrak{p}_h) - \theta(\mathfrak{p}'_1) - \cdots - \theta(\mathfrak{p}'_h)| > \frac{1}{7|\mathfrak{p}_1\cdots\mathfrak{p}_h\mathfrak{p}'_1\cdots\mathfrak{p}'_h|} \ge h/x,$$

which is a contradiction.

We observe that for each prime $p \equiv 1 \pmod 4$ there is a Gaussian prime $\mathfrak{p}$ with $|\mathfrak{p}| = \sqrt{p}$ and $\theta(\mathfrak{p}) \in (0, 1/8)$. Thus,

$$|\mathcal{A}| = \#\left\{p : \ p \equiv 1 \pmod 4,\ p \le \left(\frac{x}{7h}\right)^{\frac{1}{h}}\right\}$$

and the Prime Number Theorem for arithmetic progressions implies that

$$|\mathcal{A}| \sim \frac{\left(\frac{x}{7h}\right)^{\frac{1}{h}}}{2\log(\left(\frac{x}{7h}\right)^{\frac{1}{h}})} \gg x^{1/h}/\log x.$$

□

1.3. Proof of Theorem 1.1

Theorem 1.1 *For $h = 2, 3, 4$ there is an infinite B_h sequence $\mathcal{B}$ with counting function*

$$\mathcal{B}(x) = x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}.$$

We start following the lines of [**?**] with several adjustments. In the sequel we will write $\mathfrak{p}$ for a Gaussian prime in the first octant $(0 < \theta(\mathfrak{p}) < 1/8)$.

We fix a number $c_h > h$ which will determine the growth of the sequence we construct. Indeed $c_h = \sqrt{(h-1)^2+1} + (h-1)$ will be taken in the last step of the proof.

1.3.1. The construction

We will construct for each $\alpha \in [1,2]$ a sequence of positive integers indexed with the Gaussian primes

$$\mathcal{B}_\alpha := \{b_\mathfrak{p}\},$$

where each $b_\mathfrak{p}$ will be built using the expansion in base 2 of $\alpha\,\theta(\mathfrak{p})$:

$$\alpha\,\theta(\mathfrak{p}) = \sum_{i=1}^{\infty} \delta_{i\mathfrak{p}} 2^{-i} \qquad (\delta_{i\mathfrak{p}} \in \{0,1\}).$$

The role of the parameter α will be clear at a later stage, for the moment it is enough to note that the set $\{\alpha\theta(\mathfrak{p})\}$ obviously keeps the same B_h property as the set $\{\theta(\mathfrak{p})\}$.

To organize the construction we describe the sequence $\mathcal{B}_\alpha$ as a union of finite sets according to the sizes of the primes:

$$\mathcal{B}_\alpha = \bigcup_{K \ge h+1} \mathcal{B}_{\alpha,K},$$

where K is an integer and

$$\mathcal{B}_{\alpha,K} = \{b_\mathfrak{p} : \ \mathfrak{p} \in P_K\},$$

with

$$P_K := \{\mathfrak{p} : \ 2^{\frac{(K-2)^2}{c_h}} < |\mathfrak{p}|^2 \le 2^{\frac{(K-1)^2}{c_h}}\}.$$

Now we build the positive integers $b_\mathfrak{p} \in \mathcal{B}_{\alpha,K}$. For any $\mathfrak{p} \in P_K$ let $\widehat{\alpha\theta(\mathfrak{p})}$ denote the truncated series of $\alpha\,\theta(\mathfrak{p})$ at the K^2-place:

$$\widehat{\alpha\theta(\mathfrak{p})} := \sum_{i=1}^{K^2} \delta_{i\mathfrak{p}} 2^{-i}. \tag{1.4}$$

Combining the digits at places $(j-1)^2+1, \cdots, j^2$ into a single number

$$\Delta_{j\mathfrak{p}} = \sum_{i=(j-1)^2+1}^{j^2} \delta_{i\mathfrak{p}} 2^{j^2-i} \quad (j = 1, \cdots, K),$$

we can write

$$\widehat{\alpha\,\theta(\mathfrak{p})} = \sum_{j=1}^{K} \Delta_{j\mathfrak{p}} 2^{-j^2}. \tag{1.5}$$

We observe that if $\mathfrak{p} \in P_K$ then

$$|\widehat{\alpha\,\theta(\mathfrak{p})} - \alpha\,\theta(\mathfrak{p})| \le 2^{-K^2}. \tag{1.6}$$

The definition of $b_{\mathfrak{p}}$ is informally outlined as follows. We consider the series of blocks $\Delta_{1\mathfrak{p}}, \cdots, \Delta_{K\mathfrak{p}}$ and re-arrange them opposite to the original left to right arrangement. Then we insert at the left of each $\Delta_{j\mathfrak{p}}$ an additional filling block of $2d+1$ digits, with $d = \lceil \log_2 h \rceil$. At the filling blocks the digits will be always 0 but for an only exception: the leftmost filling block contains one digit digit 1 which marks the subset P_K the prime $\mathfrak{p}$ belongs to.

$$\alpha\,\theta(\mathfrak{p}) = 0.\overbrace{1}^{\Delta_1}\overbrace{001}^{\Delta_2}\ldots\overbrace{1\cdots\cdots 0}^{\Delta_j}\ldots\overbrace{01\cdots\cdots\cdots 11}^{\Delta_K}\underset{\underset{K^2}{\uparrow}}{\ldots}\ldots$$

$$b_{\mathfrak{p}} \leftrightarrow 0^{(d)}10^{(d)}\Delta_K 0^{(2d+1)}\Delta_{K-1}\cdots 0^{(2d+1)}\Delta_2 0^{(2d+1)}\Delta_1,$$

where $0^{(m)}$ means a string of m consecutive zeroes and Δ_i denotes the sequence of digits in the definition of $\Delta_{i\mathfrak{p}}$. The reason to add the blocks of zeroes and the value of d will be clarified just before Lemma 1.2.

More formally, for $\mathfrak{p} \in P_K$ we define

$$t_{\mathfrak{p}} = 2^{K^2+(2d+1)(K-1)+(d+1)}, \tag{1.7}$$

and

$$b_{\mathfrak{p}} = t_{\mathfrak{p}} + \sum_{j=1}^{K} \Delta_{j\mathfrak{p}} 2^{(j-1)^2+(2d+1)(j-1)}.$$

Furthermore we define $\Delta_{j\mathfrak{p}} = 0$ for $j > K$.

Remark 1.1. *The construction in [**?**] was based on the numbers $\alpha \log p$, with p rational prime, hence the digits of their integral parts had to be also included in the corresponding integers b_p. Ruzsa solved this problem by reserving fixed places for these digits. Since in our construction the integral part of $\alpha\theta(\mathfrak{p})$ is zero there is no need to care about it.*

We observe that distinct primes $\mathfrak{p}, \mathfrak{q}$ provide distinct $b_{\mathfrak{p}}, b_{\mathfrak{q}}$. Indeed if $b_{\mathfrak{p}} = b_{\mathfrak{q}}$ then $\Delta_{i\mathfrak{p}} = \Delta_{i\mathfrak{q}}$ for all $i \le K$. Also $t_{\mathfrak{p}} = t_{\mathfrak{q}}$ which means $\mathfrak{p}, \mathfrak{q} \in P_K$, and so

$$|\theta(\mathfrak{p}) - \theta(\mathfrak{q})| = \alpha^{-1} \cdot \sum_{j>K} (\Delta_{j\mathfrak{p}} - \Delta_{j\mathfrak{q}}) < 2^{-K^2}.$$

Now if $\mathfrak{p} \neq \mathfrak{q}$ then Lemma 1.1 implies that $|\theta(\mathfrak{p}) - \theta(\mathfrak{q})| > \frac{1}{7|\mathfrak{p}\mathfrak{q}|} > 2^{-\frac{1}{c}(K-1)^2-3}$. Combining both inequalities we have a contradiction for $K \ge h+1$.

Since all the integers $b_{\mathfrak{p}}$ are distinct, we have that

$$|\mathcal{B}_{\alpha,K}| = |P_K| = \pi\big(2^{\frac{(K-1)^2}{c_h}}; 1, 4\big) - \pi\big(2^{\frac{(K-2)^2}{c_h}}; 1, 4\big) \gg K^{-2} 2^{\frac{K^2}{c_h}}, \tag{1.8}$$

where $\pi(x; 1, 4)$ counts the primes not greater than x that are congruent with 1 modulus 4. Note also that

$$b_{\mathfrak{p}} < 2^{K^2+(2d+1)K+(d+1)+1}.$$

Using these estimates we can easily prove that $\mathcal{B}_\alpha(x) = x^{\frac{1}{c_h}+o(1)}$. Indeed, if K is the integer such that

$$2^{K^2+(2d+1)K+(d+1)+1} < x \le 2^{(K+1)^2+(2d+1)(K+1)+(d+1)+1}$$

then we have

$$\mathcal{B}_\alpha(x) \ge |\mathcal{B}_{\alpha,K}| = 2^{\frac{1}{c_h}K^2(1+o(1))} = x^{\frac{1}{c_h}+o(1)}. \tag{1.9}$$

For the upper bound we have

$$\mathcal{B}_\alpha(x) \le \# \left\{ \mathfrak{p} : \ |\mathfrak{p}|^2 \le 2^{\frac{K^2}{c_h}} \right\} \le 2^{\frac{K^2}{c_h}} = x^{\frac{1}{c_h}+o(1)}.$$

There is a trade-off in the choice of a particular value of c_h for the construction. On one hand larger values of c_h capture more information from the Gaussian arguments which brings the sequence $\mathcal{B}_\alpha = \{b_{\mathfrak{p}}\}$ closer to being a B_h sequence. On the other hand smaller values of c_h provide higher growth of the counting function of $\mathcal{B}_\alpha$.

Clearly $\mathcal{B}_\alpha$ would be a B_h sequence if for all $l = 2, \cdots, h$ it does not contain $b_{\mathfrak{p}_1}, \cdots, b_{\mathfrak{p}_l}, b_{\mathfrak{p}'_1}, \cdots, b_{\mathfrak{p}'_l}$ satisfying

$$\begin{aligned} b_{\mathfrak{p}_1} + \cdots + b_{\mathfrak{p}_l} \quad &= \quad b_{\mathfrak{p}'_1} + \cdots + b_{\mathfrak{p}'_l}, && (1.10)\\ \{b_{\mathfrak{p}_1}, \cdots, b_{\mathfrak{p}_l}\} \quad &\cap \quad \{b_{\mathfrak{p}'_1}, \cdots, b_{\mathfrak{p}'_l}\} = \emptyset, \\ b_{\mathfrak{p}_1} \ge \cdots \ge b_{\mathfrak{p}_l} \quad &\text{and} \quad b_{\mathfrak{p}'_1} \ge \cdots \ge b_{\mathfrak{p}'_l}. && (1.11) \end{aligned}$$

We say that $(\mathfrak{p}_1, \ldots, \mathfrak{p}_l, \mathfrak{p}'_1, \ldots, \mathfrak{p}'_l)$ is a *bad* $2l$-tuple if the equation 1.10 is satisfied by the corresponding $b_{\mathfrak{p}_r}, b_{\mathfrak{p}'_r} (1 \le r \le l)$.

The sequence $\mathcal{B}_\alpha = \{b_\mathfrak{p}\}$ we have constructed so far is not a B_h sequence yet. Some repeated sums as in (1.10) will eventually appear, however the precise way how the elements $b_\mathfrak{p}$ are built will allow us to study these bad $2l$-tuples in order to prove that there are not too many repeated sums. Then after removing the bad elements involved in these bad $2l$-tuples we will obtain a true B_h sequence.

Now we will see why blocks of zeroes were added to the binary expansion of $b_\mathfrak{p}$. We can identify each $b_\mathfrak{p}$, with $\mathfrak{p} \in P_K$, with a vector as follows:

$$b_\mathfrak{p} \leftrightarrow (0^\infty, 1, 0^{(d)}, \Delta_K, 0^{(2d+1)}, \Delta_{K-1}, \ldots, 0^{(2d+1)}, \Delta_2, 0^{(2d+1)}, \Delta_1),$$

where $0^{(m)}$ means a string of m consecutive zeroes and Δ_i denotes the sequence of digits in the definition of $\Delta_{i\mathfrak{p}}$. Note that the leftmost part of each vector is null. The value of $d = \lceil \log_2 h \rceil$ has been chosen to prevent the propagation of the carry between any two consecutive coordinates separated by a comma in the above identification. So when we sum no more than h integers $b_\mathfrak{p}$ we can just sum the corresponding vectors coordinate-wise. This fact is used in the following lemma.

Lemma 1.2. *Let* $(\mathfrak{p}_1, \cdots, \mathfrak{p}_l, \mathfrak{p}'_1, \cdots, \mathfrak{p}'_l)$ *be a bad* $2l$*-tuple. Then there are integers* $K_1 \ge \cdots \ge K_l$ *such that* $\mathfrak{p}_1, \mathfrak{p}'_1 \in P_{K_1}, \cdots, \mathfrak{p}_l, \mathfrak{p}'_l \in P_{K_l}$, *and we have*

$$\widehat{\alpha\theta(\mathfrak{p}_1)} + \cdots + \widehat{\alpha\theta(\mathfrak{p}_l)} = \widehat{\alpha\theta(\mathfrak{p}'_1)} + \cdots + \widehat{\alpha\theta(\mathfrak{p}'_l)}. \tag{1.12}$$

Proof. Note that (1.10) implies $t_{\mathfrak{p}_1} + \cdots + t_{\mathfrak{p}_l} = t_{\mathfrak{p}'_1} + \cdots + t_{\mathfrak{p}'_l}$ and $\Delta_{j\mathfrak{p}_1} + \cdots + \Delta_{j\mathfrak{p}_l} = \Delta_{j\mathfrak{p}'_1} + \cdots + \Delta_{j\mathfrak{p}'_l}$ for each j. Using (1.5) we conclude (1.12). As the bad $2l$-tuple satisfies condition (1.11) we deduce that $\mathfrak{p}_r, \mathfrak{p}'_r$ belong to the same P_{K_r} for all r. □

According to the previous lemma we will write $E_{2l}(\alpha; K_1, \cdots, K_l)$ for the set of bad $2l$-tuples $(\mathfrak{p}_1, \cdots, \mathfrak{p}'_l)$ with $\mathfrak{p}_r, \mathfrak{p}'_r \in P_{K_r},\ 1 \le r \le l$ and

$$E_{2l}(\alpha; K) = \bigcup_{K_l \le \cdots \le K_1 = K} E_{2l}(\alpha; K_1, \cdots, K_l),$$

where $K = K_1$. Also we define the set

$\mathrm{Bad}_{\alpha,K} = \{b_{\mathfrak{p}} \in \mathcal{B}_{\alpha,K} :\ b_{\mathfrak{p}}$ is the largest element involved in some equation (1.10)$\}$.

It is clear that $\sum_{l\le h} |E_{2l}(\alpha, K)|$ is an upper bound for $|\mathrm{Bad}_{\alpha,K}|$, the number of elements we need to remove from each $\mathcal{B}_{\alpha,K}$ to get a B_h sequence:

$$|\mathrm{Bad}_{\alpha,K}| \le \sum_{l\le h} |E_{2l}(\alpha, K)|. \tag{1.13}$$

We do not know how to obtain a good upper bound for $|E_{2l}(\alpha, K)|$ for a particular α, however we can do it for almost all α.

Lemma 1.3. *For $l = 2, 3, 4$ and $c_h > h \ge l$ we have*

$$\int_1^2 |E_{2l}(\alpha, K)|\, \mathrm{d}\alpha \ll K^{m_l} 2^{\left(\frac{2(l-1)}{c_h-1}-1\right)(K-1)^2-2K},$$

for some m_l.

The proof this lemma is involved and we postpone it to §1.4.

1.3.2. Last step in the proof of Theorem 1.1

For $h = 2, 3, 4$ we use (1.13) and (1.8) to get

$$\begin{aligned}
\int_1^2 \frac{|\mathrm{Bad}_{\alpha,K}|}{|\mathcal{B}_{\alpha,K}|}\, \mathrm{d}\alpha &\ll \frac{\sum_{l\le h} \int_1^2 |E_{2l}(\alpha, K)|\, \mathrm{d}\alpha}{K^{-2} 2^{\frac{1}{c_h}(K-1)^2}} \\
&\ll \frac{\sum_{l\le h} K^{m_l} 2^{\left(\frac{2(l-1)}{c_h-1}-1\right)(K-1)^2-2K}}{K^{-2} 2^{\frac{1}{c_h}(K-1)^2}} \\
&\ll K^{m_l+2} 2^{\left(\frac{2(h-1)}{c_h-1}-1-\frac{1}{c_h}\right)(K-1)^2-2K} \\
&\ll K^{m_l+2} 2^{-2K}
\end{aligned}$$

for $c_h = \sqrt{(h-1)^2+1} + (h-1)$ which is the smallest number c satisfying the inequality $\frac{2(h-1)}{c-1} - 1 - \frac{1}{c} \le 0$. So for this c_h the sum $\sum_K \int_1^2 \frac{|\mathrm{Bad}_{\alpha,K}|}{|\mathcal{B}_{\alpha,K}|}\, \mathrm{d}\alpha$ is convergent and then we have that $\int_1^2 \sum_K \frac{|\mathrm{Bad}_{\alpha,K}|}{|\mathcal{B}_{\alpha,K}|}\, \mathrm{d}\alpha$ is finite. So $\sum_K \frac{|\mathrm{Bad}_{\alpha,K}|}{|\mathcal{B}_{\alpha,K}|}$

is convergent for almost all $\alpha \in [1,2]$. We take one of these α, say α_0, and consider the sequence

$$\mathcal{B} = \bigcup_K \left(\mathcal{B}_{\alpha_0,K} \setminus \mathrm{Bad}_{\alpha_0,K}\right).$$

We claim that this sequence satisfies the condition of the theorem. On one hand this sequence clearly is a B_h sequence because we have destroyed all the repeated sums of h elements of $\mathcal{B}_{\alpha_0}$ by removing one element from each bad $2l$-tuple.

On the other hand the convergence of $\sum_K \frac{|\mathrm{Bad}_{\alpha_0,K}|}{|\mathcal{B}_{\alpha_0,K}|}$ implies that $|\mathrm{Bad}_{\alpha_0,K}| = o\left(|\mathcal{B}_{\alpha_0,K}|\right)$. We proceed as in (1.9) to estimate the counting function of $\mathcal{B}$. For any x let K be the integer such that

$$2^{K^2+(2d+1)K+(d+1)+1} < x \le 2^{(K+1)^2+(2d+1)(K+1)+(d+1)+1}.$$

We have

$$\mathcal{B}(x) \ge |\mathcal{B}_{\alpha_0,K}| - |\mathrm{Bad}_{\alpha_0,K}| = |\mathcal{B}_{\alpha_0,K}|(1+o(1)) \gg K^{-2} 2^{\frac{1}{c_h}K^2} = x^{\frac{1}{c_h}+o(1)}.$$

For the upper bound, we have

$$\mathcal{B}(x) \le \mathcal{B}_{\alpha_0}(x) = x^{\frac{1}{c_h}+o(1)}.$$

Note that $1/c_h = \sqrt{(h-1)^2+1} - (h-1)$. Hence

$$\mathcal{B}(x) = x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}.$$

1.4. Proof of Lemma 1.3

Lemma 1.3 *For $l = 2,3,4$ and $c_h > h \ge l$ we have*

$$\int_1^2 |E_{2l}(\alpha, K)|\,\mathrm{d}\alpha \ll K^{m_l} 2^{\left(\frac{2(l-1)}{c_h-1}-1\right)(K-1)^2-2K},$$

for some m_l.

The proof of Lemma 1.3 will be a consequence of Propositions 1.1, 1.2 and 1.3. Before proving these propositions we need some properties of the bad $2l$-tuples and an auxiliary lemma about visible lattice points.

1.4.1. Some properties of the 2ℓ-tuples

For any $2l$-tuple $(\mathfrak{p}_1, \cdots, \mathfrak{p}_l, \mathfrak{p}'_1, \cdots, \mathfrak{p}'_l)$ we define the numbers $\omega_s = \omega_s(\mathfrak{p}_1, \cdots, \mathfrak{p}_l, \mathfrak{p}'_1, \cdots, \mathfrak{p}'_l)$ by

$$\omega_s = \sum_{r=1}^{s} (\theta(\mathfrak{p}_r) - \theta(\mathfrak{p}'_r)) \qquad (s \leq l).$$

The next two lemmas show several properties of the bad $2l$-tuples.

Lemma 1.4. *Let $(\mathfrak{p}_1, \cdots, \mathfrak{p}_l, \mathfrak{p}'_1, \cdots, \mathfrak{p}'_l) \in E_{2l}(\alpha; K_1, \cdots, K_l)$ be a bad $2l$-tuple. We have*

$$\begin{aligned} \text{i)} \quad & |\omega_l| \leq l 2^{-K_l^2}, \\ \text{ii)} \quad & |\omega_{l-1}| \geq 2^{-\frac{1}{c_h}(K_l-1)^2-4}, \\ \text{iii)} \quad & (K_l - 1)^2 \leq \frac{(K_1-1)^2 + \cdots + (K_{l-1}-1)^2}{c_h - 1}. \end{aligned}$$

Proof. i) This is a consequence of (1.12) and (1.6):

$$|\omega_l| = \frac{1}{\alpha} \left| \sum_{r=1}^{l} (\alpha\theta(\mathfrak{p}_r) - \alpha\theta(\mathfrak{p}'_r)) \right| \leq \frac{1}{\alpha} \left(2^{-K_1^2} + \cdots + 2^{-K_l^2} \right) \leq l 2^{-K_l^2}.$$

ii) Lemma 1.1 implies

$$|\theta(\mathfrak{p}_l) - \theta(\mathfrak{p}'_l)| \geq \frac{1}{7\,|\mathfrak{p}_l \mathfrak{p}'_l|} \geq 2^{-3-\frac{1}{c_h}(K_l-1)^2}, \tag{1.14}$$

and so

$$\begin{aligned} |\omega_{l-1}| &= |\omega_l + \theta(\mathfrak{p}'_l) - \theta(\mathfrak{p}_l)| \geq |\theta(\mathfrak{p}'_l) - \theta(\mathfrak{p}_l)| - |\omega_l| \\ &\geq 2^{-\frac{1}{c_h}(K_l-1)^2-3} - l 2^{-K_l^2} \geq 2^{-\frac{1}{c_h}(K_l-1)^2-4}, \end{aligned}$$

since $K_l \geq h+1 \geq l+1$.

iii) Lema 1.1 also implies that

$$|\omega_l| = \left| \sum_{r=1}^{l} (\theta(\mathfrak{p}_r) - \theta(\mathfrak{p}'_r)) \right| > \frac{1}{7\,|\mathfrak{p}_1 \cdots \mathfrak{p}'_l|} > 2^{-3-\frac{1}{c_h}\sum_{r=1}^{l}(K_r-1)^2}.$$

Combining this with i) we obtain

$$(K_l - 1)^2 \leq \frac{1}{c_h - 1} \left((K_1-1)^2 + \cdots + (K_{l-1}-1)^2 \right) + \frac{\log_2 l - 2K_l + 4}{1 - 1/c_h}.$$

The last term is negative because $K_l \geq h+1 \geq l+1$ and $l \geq 2$. $\square$

Lemma 1.5. *Let* $(\mathfrak{p}_1, \cdots, \mathfrak{p}_l, \mathfrak{p}'_1, \cdots, \mathfrak{p}'_l) \in E_{2l}(\alpha; K_1, \cdots, K_l)$ *be a bad* $2l$*-tuple. Then for any* $\omega_s = \sum_{r=1}^{s} (\theta(\mathfrak{p}_r) - \theta(\mathfrak{p}'_r))$ *with* $1 \le s \le l-1$ *we have*

$$\left\| \alpha 2^{K_{s+1}^2} \omega_s \right\| \le s 2^{K_{s+1}^2 - K_s^2} \qquad (s = 1, \cdots, l-1), \tag{1.15}$$

where $\|\cdot\|$ *means the distance to the nearest integer.*

Proof. Since $0 \le \alpha\theta(\mathfrak{p}) - \widehat{\alpha\theta(\mathfrak{p})} \le 2^{-K^2}$ when $\mathfrak{p} \in P_K$, then

$$|\,(\theta(\mathfrak{p}_r) - \theta(\mathfrak{p}'_r)) - \left(\widehat{\alpha\theta(\mathfrak{p}_r)} - \widehat{\alpha\theta(\mathfrak{p}'_r)}\right)| \le 2^{-K_s^2}$$

for any $\mathfrak{p}_r, \mathfrak{p}'_r \in K_r$ with $r \le s$ and we can write

$$2^{K_{s+1}^2} \alpha \sum_{r=1}^{s} (\theta(\mathfrak{p}_r) - \theta(\mathfrak{p}'_r)) = 2^{K_{s+1}^2} \sum_{r=1}^{s} \left(\widehat{\alpha\theta(\mathfrak{p}_r)} - \widehat{\alpha\theta(\mathfrak{p}'_r)}\right) + \epsilon_s,$$

with $|\epsilon_s| \le s 2^{K_{s+1}^2 - K_s^2}$. By the definition (1.4) of $\widehat{\alpha\theta(\mathfrak{p})}$ we have,

$$2^{K_{s+1}^2} \sum_{r=s+1}^{l} \left(\widehat{\alpha\theta(\mathfrak{p}'_r)} - \widehat{\alpha\theta(\mathfrak{p}_r)}\right) = \sum_{r=s+1}^{l} \sum_{i=1}^{K_r^2} 2^{K_{s+1}^2 - i} (\delta_{i\mathfrak{p}'_r} - \delta_{i\mathfrak{p}_r})$$

which is an integer. By Lemma 1.2 we know that $\sum_{r=1}^{l} \left(\widehat{\alpha\theta(\mathfrak{p}_r)} - \widehat{\alpha\theta(\mathfrak{p}'_r)}\right) = 0$. It follows that

$$\|2^{K_{s+1}^2} \omega_s\| = |\epsilon_s| \le s 2^{K_{s+1}^2 - K_s^2},$$

as claimed. □

Lemma 1.6.

$$\int_1^2 |E_{2l}(\alpha; K_1, \cdots, K_l)|\, \mathrm{d}\alpha \ll 2^{K_l^2 - K_1^2} \sum_{\substack{(\mathfrak{p}_1, \cdots, \mathfrak{p}'_l) \\ |\omega_l| < l \cdot 2^{-K_l^2}}} \frac{|\omega_{l-1}|}{|\omega_1|} \prod_{j=1}^{l-2} \left(\frac{|\omega_j|}{|\omega_{j+1}|} + 1 \right)$$

Proof. We know by Lemma 1.4 i)) that if $(\mathfrak{p}_1, \cdots, \mathfrak{p}'_l) \in E_{2l}(\alpha; K_1, \cdots, K_l)$, then $|\omega_l| < l 2^{-K_l^2}$. Thus

$$\int_1^2 |E_{2l}(\alpha; K_1, \cdots, K_l)|\, \mathrm{d}\alpha \le \sum_{\substack{(\mathfrak{p}_1, \cdots, \mathfrak{p}'_l) \\ |\omega_l| < l \cdot 2^{-K_l^2}}} \mu\{\alpha : \ (\mathfrak{p}_1, \cdots, \mathfrak{p}'_l) \in E_{2l}(\alpha; K_1, \cdots, K_l)\}. \tag{1.16}$$

We have seen that if $(\mathfrak{p}_1, \cdots, \mathfrak{p}_l') \in E_{2l}(\alpha; K_1, \cdots, K_l)$, then

$$\left\|\alpha 2^{K_{s+1}^2}\omega_s\right\| \leq s 2^{K_{s+1}^2-K_s^2}, \; s = 1, \ldots, l-1. \tag{1.17}$$

Then there exist integers j_s, $s = 1, \cdots, l-1$ such that

$$\left|\alpha 2^{K_{s+1}^2}\omega_s - j_s\right| \leq s 2^{K_{s+1}^2-K_s^2}, \tag{1.18}$$

so

$$\left|\alpha - \frac{j_s}{2^{K_{s+1}^2}\omega_s}\right| \leq \frac{s 2^{-K_s^2}}{|\omega_s|}. \tag{1.19}$$

Writing $I_{j_1}, \cdots, I_{j_s}$ for the intervals defined by the inequalities (1.19), we have

$$\begin{aligned} \mu\{\alpha : \; (\mathfrak{p}_1, \cdots, \mathfrak{p}_l') \in E_{2l}(\alpha; K_1, \cdots, K_l)\} &\leq \sum_{j_1, \cdots, j_{l-1}} \left|I_{j_1} \cap \cdots \cap I_{j_{l-1}}\right| \\ &\leq \frac{2^{-K_1^2+1}}{|\omega_1|} \#\{(j_1, \ldots, j_{l-1}) : \bigcap_{i=1}^{l-1} I_{j_i} \neq \emptyset\} \end{aligned} \tag{1.20}$$

To estimate this last cardinal note that for all $s = 1, \cdots, l-2$ we have

$$\begin{aligned} \left|\frac{j_s}{2^{K_{s+1}^2}\omega_s} - \frac{j_{s+1}}{2^{K_{s+2}^2}\omega_{s+1}}\right| &< \left|\alpha - \frac{j_s}{2^{K_{s+1}^2}\omega_s}\right| + \left|\alpha - \frac{j_{s+1}}{2^{K_{s+2}^2}\omega_{s+1}}\right| \\ &< \frac{s 2^{-K_s^2}}{|\omega_s|} + \frac{(s+1) 2^{-K_{s+1}^2}}{|\omega_{s+1}|}. \end{aligned}$$

Thus

$$\left|j_s - j_{s+1}\frac{2^{K_{s+1}^2}\omega_s}{2^{K_{s+2}^2}\omega_{s+1}}\right| < s 2^{-K_s^2+K_{s+1}^2} + \frac{(s+1)|\omega_s|}{|\omega_{s+1}|}. \tag{1.21}$$

We observe that for each $s = 1, \cdots, l-2$ and for each j_{s+1}, the number of j_s satisfying (1.21) is bounded by $2\left(s 2^{-K_s^2+K_{s+1}^2} + \frac{(s+1)|\omega_s|}{|\omega_{s+1}|}\right) + 1 \ll \frac{|\omega_s|}{|\omega_{s+1}|} + 1$.

Note also that (1.18) for $s = l-1$ implies

$$\begin{aligned} |j_{l-1}| &\leq \alpha 2^{K_l^2}\omega_{l-1} + (l-1) 2^{K_l^2-K_{l-1}^2} \\ &\leq 2^{K_l^2+1}\omega_{l-1} + (l-1) \\ &\ll 2^{K_l^2}\omega_{l-1}. \end{aligned}$$

Thus,

$$\#\{(j_1,\dots,j_{l-1}) : \bigcap_{i=1}^{l-1} I_{j_i} \neq \emptyset\} \ll 2^{K_l^2}\omega_{l-1}\prod_{s=1}^{l-2}\left(\frac{|\omega_s|}{|\omega_{s+1}|}+1\right). \tag{1.22}$$

The proof can be completed putting (1.22) in (1.20) and then in (1.16). □

1.4.2. Visible points

We will denote by $\mathcal{V}$ the set of points in the integer two dimensional lattice $\mathbb{Z}^2$ visible from the origin except $(1,0)$. In the next subsection we will use several times the following lemma.

Lemma 1.7. *The number of points in $\mathcal{V}$ that are contained in a circular sector centred at the origin of radius R and angle ϵ is at most ϵR^2+1. In other words, for any real number t*

$$\#\{\nu \in \mathcal{V},\ |\nu| < R,\ \|\theta(\nu)+t\| < \epsilon\} \le \epsilon R^2 + 1.$$

Furthermore,

$$\#\{\nu \in \mathcal{V},\ |\nu| < R,\ \|\theta(\nu)\| < \epsilon\} \le \epsilon R^2.$$

Proof. We order the N points inside de sector $\nu_1,\nu_2,\cdots,\nu_N \in \mathcal{V}$ by the value of their argument so that $\theta(\nu_i) < \theta(\nu_j)$ for $1 \le i < j \le N$. For each $i = 1,\dots,N-1$ the three lattice points O,ν_i,ν_{i+1} define a triangle T_i with $\text{Area}(T_i) \ge 1/2$, that does not contain any other lattice point.

Since all T_i are inside the circular sector their union covers at most the area of the sector. Their interiors are pairwise disjoint, thus

$$N-1 \le \sum_{i=1}^{N} 2\cdot \text{Area}(T_i) = 2\cdot \text{Area}\left(\bigcup_{i=1}^{N} T_i\right) \le R^2\epsilon.$$

For the last statement we add $\nu_0 = (1,0)$ to the points $\nu_1,\dots,\nu_N$ and we repeat the argument. □

1.4.3. Estimates for the number of bad 2ℓ-tuples ($\ell = 2, 3, 4$)

We start with the case $l = 2$ which was considered by Ruzsa for B_2 sequences. In the sequel all lattice points ν appearing in the proofs belong to $\mathcal{V}$ and Lemma 1.7 applies.

Proposition 1.1. *For any $c_h > 2$ we have*

$$\int_1^2 |E_4(\alpha; K)|\,\mathrm{d}\alpha \ll K \cdot 2^{\left(\frac{2}{c_h-1}-1\right)(K-1)^2-2K}.$$

Proof. Lemma 1.6 implies that

$$\int_1^2 |E_4(\alpha; K_1, K_2)|\,\mathrm{d}\alpha \ll 2^{K_2^2-K_1^2}\,\#\{(\mathfrak{p}_1, \mathfrak{p}_1', \mathfrak{p}_2, \mathfrak{p}_2') \colon |\omega_2| \le 2 \cdot 2^{-K_2^2}\}.$$

We get an upper bound for the second factor here by using Lemma 1.7 to estimate the number of lattice points of the form $\nu_2 = \mathfrak{p}_1\mathfrak{p}_1'\overline{\mathfrak{p}_2\mathfrak{p}_2'}$ such that

$$|\omega_2| = \|\theta(\nu_2)\| < \epsilon,\ |\nu_2| < R \quad \text{with} \quad \epsilon = 2{\cdot}2^{-K_2^2} \quad \text{and} \quad R = 2^{\frac{1}{c_h}((K_1-1)^2+(K_2-1)^2)}.$$

We have

$$\begin{aligned}\int_1^2 |E_4(\alpha; K_1, K_2)|\,\mathrm{d}\alpha &\ll 2^{K_2^2-K_1^2} \cdot 2^{\frac{2}{c_h}((K_1-1)^2+(K_2-1)^2)-K_2^2} \\ &\ll 2^{\frac{2}{c_h}((K_1-1)^2+(K_2-1)^2)-K_1^2}.\end{aligned}$$

By Lemma 1.4 iii) we also have $(K_2-1)^2 \le \frac{(K_1-1)^2}{c_h-1}$, thus

$$\int_1^2 |E_4(\alpha; K_1, K_2)|\,\mathrm{d}\alpha \ll 2^{\left(\frac{2}{c_h-1}-1\right)K_1^2-2K_1}$$

and

$$\begin{aligned}\int_1^2 |E_4(\alpha; K)|\,\mathrm{d}\alpha &= \sum_{K_2 \le K} \int_1^2 |E_4(\alpha; K, K_2)|\,\mathrm{d}\alpha \\ &\ll K \cdot 2^{\left(\frac{2}{c_h-1}-1\right)(K-1)^2-2K}.\end{aligned}$$

□

Proposition 1.2. *For any $c_h > 3$ we have*

$$\int_1^2 |E_6(\alpha;K)|\,\mathrm{d}\alpha \ll K^4\, 2^{\left(\frac{4}{c_h-1}-1\right)(K-1)^2-2K}.$$

Proof. Lemma 1.6 says that

$$\int_1^2 |E_6(\alpha;K_1,K_2,K_3)|\,\mathrm{d}\alpha \ll 2^{K_3^2-K_1^2} \sum_{\substack{(\mathfrak{p}_1,\cdots,\mathfrak{p}_3')\\ |\omega_3|\le 3\cdot 2^{-K_3^2}}} \frac{1}{|\omega_1|}.$$

Since $|\omega_1| = \|\theta(\mathfrak{p}_1\overline{\mathfrak{p}_1'})\| \ge 2^{-3-\frac{(K_1-1)^2}{c_h}}$ we split the sum above according $|\omega_1| \le 2^{-m}$ for $m \le M = 3 + (K_1-1)^2/c_h$. Summing for all m in this range and applying Lemma 1.7 with $\nu_1 = \mathfrak{p}_1\overline{\mathfrak{p}_1'}$ and $\nu_2 = \mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}_2'\mathfrak{p}_3'}$, we have that

$$\begin{aligned}
\sum_{\substack{(\mathfrak{p}_1,\cdots,\mathfrak{p}_3')\\ |\omega_3|\le 3\cdot 2^{-K_3^2}}} \frac{1}{|\omega_1|} &\ll \sum_{m\le M} 2^m \#\{(\mathfrak{p}_1,\cdots,\mathfrak{p}_3') :\ |\omega_1| \le 2^{-m}, |\omega_3| \le 3\cdot 2^{-K_3^2}\} \\
&\ll \sum_{m\le M} 2^m \#\{(\nu_1,\nu_2) :\ \|\theta(\nu_1)\| \le 2^{-m},\ \|\theta(\nu_1)+\theta(\nu_2)\| \le 3\cdot 2^{-K_3^2}\} \\
&\ll \sum_{m\le M} 2^m \sum_{|\theta(\nu_1)|\le 2^{-m}} \#\{\nu_2 :\ \|\theta(\nu_1)+\theta(\nu_2)\| \le 3\cdot 2^{-K_3^2}\} \\
&\ll \sum_{m\le M} 2^m \cdot 2^{\frac{2}{c_h}(K_1-1)^2-m} \left(2^{\frac{2}{c_h}\left((K_2-1)^2+(K_3-1)^2\right)-K_3^2} + 1\right).
\end{aligned}$$

Hence using the inequalities $K_3 \le K_2 \le K_1$ and $(K_3-1)^2 \le \frac{(K_2-1)^2+(K_1-1)^2}{c_h-1}$ (property iii) in Lemma 1.4) we have

$$\begin{aligned}
\int_1^2 |E_6(\alpha;K_1,K_2,K_3)|\,\mathrm{d}\alpha &\ll K_1^2 2^{K_3^2-K_1^2+\frac{2}{c_h}(K_1-1)^2} \left(2^{\frac{2}{c_h}\left((K_2-1)^2+(K_3-1)^2\right)-K_3^2} + 1\right) \\
&\ll K_1^2 2^{-K_1^2+\frac{2}{c_h}\left((K_1-1)^2+(K_2-1)^2+(K_3-1)^2\right)} + K_1^2 2^{K_3^2-K_1^2+\frac{2}{c_h}(K_1-1)^2} \\
&\ll K_1^2 2^{-(K_1-1)^2+\frac{2}{c_h}\left((K_1-1)^2+(K_2-1)^2+(K_3-1)^2\right)-2K_1} \\
&\quad + \quad K_1^2 2^{(K_3-1)^2-(K_1-1)^2+\frac{2}{c_h}(K_1-1)^2} \\
&\ll K_1^2 2^{\left(\frac{4}{c_h-1}-1\right)(K_1-1)^2-2K_1} + K_1^2 2^{\left(\frac{4}{c_h-1}-1\right)(K_1-1)^2-\frac{2}{c_h(c_h-1)}(K_1-1)^2} \\
&\ll K_1^2 2^{\left(\frac{4}{c_h-1}-1\right)(K_1-1)^2-2K_1}.
\end{aligned}$$

Then we can write

$$\int_1^2 |E_6(\alpha;K)|\,\mathrm{d}\alpha = \sum_{K_3\le K_2\le K}\int_1^2 |E_6(\alpha;K,K_2,K_3)|\,\mathrm{d}\alpha \ll K^4 2^{\left(\frac{4}{c-1}-1\right)(K-1)^2-2K},$$

as claimed. □

Proposition 1.3. *For any $c_h>4$ we have*

$$\int_1^2 |E_8(\alpha;K)|\,\mathrm{d}\alpha \ll K^5\, 2^{(\frac{6}{c_h-1}-1)(K-1)^2-2K}.$$

Proof. Considering the two possibilities $|\omega_1|<|\omega_2|$ and $|\omega_1|\ge|\omega_2|$ we get the inequality

$$\frac{|\omega_3|}{|\omega_1|}\left(\frac{|\omega_1|}{|\omega_2|}+1\right)\left(\frac{|\omega_2|}{|\omega_3|}+1\right) \ll \frac{|\omega_3|}{|\omega_1|}\left(\frac{|\omega_1|}{|\omega_2|}+1\right)\frac{1}{|\omega_3|} \ll \max\left(\frac{1}{|\omega_1|},\frac{1}{|\omega_2|}\right).$$

This combined with Lemma 1.6 implies that

$$\int_1^2 |E_8(\alpha,K_1,K_2,K_3,K_4)|\,\mathrm{d}\alpha \;\ll\; 2^{-K_1^2+K_4^2}\left(\sum_{\substack{(\mathfrak{p}_1,\cdots,\mathfrak{p}_4')\\ |\omega_4|\le 4\cdot 2^{-K_4^2}}}\frac{1}{|\omega_1|}+\sum_{\substack{(\mathfrak{p}_1,\cdots,\mathfrak{p}_4')\\ |\omega_4|\le 4\cdot 2^{-K_4^2}}}\frac{1}{|\omega_2|}\right)$$

Applying Lemma 1.7 with the notation $\nu_1=\mathfrak{p}_1\overline{\mathfrak{p}_1'}$ and $\nu_2=\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\overline{\mathfrak{p}_2'\mathfrak{p}_3'\mathfrak{p}_4'}$ and taking again $M=3+(K_1-1)^2/c_h$, we have that

$$\begin{aligned}
\sum_{\substack{(\mathfrak{p}_1,\cdots,\mathfrak{p}_4')\\ |\omega_4|\le 4\cdot 2^{-K_4^2}}}\frac{1}{|\omega_1|} &\ll \sum_{m\le M} 2^m\#\{(\mathfrak{p}_1,\cdots,\overline{\mathfrak{p}_4}):\ |\omega_1|<2^{-m},\ |\omega_4|\le 4\cdot 2^{-K_4^2}\}\\
&\ll \sum_{m\le M} 2^m\#\{(\nu_1,\nu_2):\ \|\theta(\nu_1)\|\le 2^{-m},\ \|\theta(\nu_1)+\theta(\nu_2)\|\le 4\cdot 2^{-K_4^2}\}\\
&\ll \sum_{m\le M}\sum_{\|\theta(\nu_1)\|<2^{-m}}\#\{\nu_2:\ \|\theta(\nu_1)+\theta(\nu_2)\|\le 4\cdot 2^{-K_4^2}\}\\
&\ll \sum_{m\le M} 2^{\frac{2}{c_h}(K_1-1)^2}\left(2^{\frac{2}{c_h}((K_2-1)^2+(K_3-1)^2+(K_4-1)^2)-K_4^2}+1\right)\\
&\ll K_1^2 2^{\frac{2}{c_h}((K_1-1)^2+(K_2-1)^2+(K_3-1)^2+(K_4-1)^2)-K_4^2}+K_1^2 2^{\frac{2}{c_h}(K_1-1)^2}.
\end{aligned}$$

Similarly, but writing now $\nu_1 = \mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_1'\mathfrak{p}_2'}$ and $\nu_2 = \mathfrak{p}_3\mathfrak{p}_4\overline{\mathfrak{p}_3'\mathfrak{p}_4'}$ we have

$$\begin{aligned}
\sum_{\substack{(\mathfrak{p}_1,\cdots,\mathfrak{p}_4')\\ |\omega_4|\le 4\cdot 2^{-K_4^2}}} \frac{1}{|\omega_2|} &\ll \sum_{m\le M} 2^m \#\{(\mathfrak{p}_1,\cdots,\overline{\mathfrak{p}_4}):\ |\omega_2|\le 2^{-m},\ |\omega_4|\le 4\cdot 2^{-K_4^2}\} \\
&\ll \sum_{m\le K_4^2} 2^m \#\{(\nu_1,\nu_2):\ \|\theta(\nu_1)\|\le 2^{-m},\ \|\theta(\nu_1)+\theta(\nu_2)\|\le 4\cdot 2^{-K_4^2}\} \\
&+ \sum_{m> K_4^2} 2^m \#\{(\nu_1,\nu_2):\ \|\theta(\nu_1)\|\le 2^{-m},\ \|\theta(\nu_1)+\theta(\nu_2)\|\le 4\cdot 2^{-K_4^2}\} \\
&= S_1+S_2.
\end{aligned}$$

We observe that if $m\le K_4^2$ then $\|\theta(\nu_2)\|\le\|\theta(\nu_1)+\theta(\nu_2)\|+\|\theta(\nu_1)\|\le 5\cdot 2^{-m}$. Thus

$$\begin{aligned}
S_1 &\ll \sum_{m\le K_4^2} 2^m \#\{(\nu_1,\nu_2):\ \|\theta(\nu_2)\|\le 5\cdot 2^{-m},\ \|\theta(\nu_1)+\theta(\nu_2)\|\le 4\cdot 2^{-K_4^2}\} \\
&\ll \sum_{m\le K_4^2} 2^m \sum_{\|\theta(\nu_2)\|\le 5\cdot 2^{-m}} \#\{\nu_1:\ \|\theta(\nu_1)+\theta(\nu_2)\|\le 4\cdot 2^{-K_4^2}\} \\
&\ll \sum_{m\le K_4^2} 2^m\cdot 2^{\frac{2}{c_h}\left((K_3-1)^2+(K_4-1)^2\right)-m}\left(2^{\frac{2}{c_h}\left((K_1-1)^2+(K_2-1)^2\right)-K_4^2}+1\right) \\
&\ll K_4^2 2^{\frac{2}{c_h}((K_1-1)^2+(K_2-1)^2+(K_3-1)^2+(K_4-1)^2)-K_4^2}+K_4^2 2^{\frac{2}{c_h}\left((K_3-1)^2+(K_4-1)^2\right)}.
\end{aligned}$$

To estimate S_2, we observe that if $m>K_4^2$ then $\|\theta(\nu_2)\|\le\|\theta(\nu_1)+\theta(\nu_2)\|+\|\theta(\nu_1)\|\le 5\cdot 2^{-K_4^2}$. Thus

$$\begin{aligned}
S_2 &\ll \sum_{K_4^2<m\le M} 2^m \#\{(\nu_1,\nu_2):\ \|\theta(\nu_1)\|\le 2^{-m},\ \|\theta(\nu_2)\|\le 5\cdot 2^{-K_4^2}\} \\
&\ll \sum_{K_4^2<m\le M} 2^m\cdot 2^{\frac{2}{c_h}\left((K_1-1)^2+(K_2-1)^2\right)-m}\cdot 2^{\frac{2}{c_h}\left((K_3-1)^2+(K_4-1)^2\right)-K_4^2} \\
&\ll K_1^2 2^{\frac{2}{c_h}((K_1-1)^2+(K_2-1)^2+(K_3-1)^2+(K_4-1)^2)-K_4^2}.
\end{aligned}$$

Putting together the estimates we have obtained for $\sum\frac{1}{|\omega_1|}$ and $\sum\frac{1}{|\omega_2|}$ we get

$$\begin{aligned}
\int_1^2 |E_8(\alpha,K_1,K_2,K_3,K_4)|\,\mathrm{d}\alpha &\ll K_1^2 2^{\frac{2}{c_h}((K_1-1)^2+(K_2-1)^2+(K_3-1)^2+(K_4-1)^2)-K_1^2} \\
&+ K_1^2 2^{-K_1^2+K_4^2+\frac{2}{c_h}(K_1-1)^2} \\
&+ K_1^2 2^{K_4^2-K_1^2+\frac{2}{c_h}\left((K_3-1)^2+(K_4-1)^2\right)} \\
&= T_1+T_2+T_3.
\end{aligned}$$

Using the inequalities $(K_4-1)^2 \leq \frac{1}{c_h-1}\left((K_1-1)^2+(K_2-1)^2+(K_3-1)^2\right)$ and $K_4 \leq K_3 \leq K_2 \leq K_1$ we have

$$T_1 \ll K_1^2 2^{\left(-1+\frac{6}{c_h-1}\right)(K_1-1)^2-2K_1},$$

$$\begin{aligned} T_2 &\ll K_1^2 2^{-(K_1-1)^2+(K_4-1)^2+\frac{2}{c_h}(K_1-1)^2} \\ &\ll K_1^2 2^{\left(-1+\frac{3}{c_h-1}+\frac{2}{c_h}\right)(K_1-1)^2} \\ &\ll K_1^2 2^{\left(-1+\frac{6}{c_h-1}\right)(K_1-1)^2-2K_1} \end{aligned}$$

and

$$\begin{aligned} T_3 &\ll K_1^2 2^{(K_4-1)^2-(K_1-1)^2+\frac{2}{c_h}\left((K_3-1)^2+(K_4-1)^2\right)} \\ &\ll K_1^2 2^{\left(1+\frac{2}{c_h}\right)\frac{1}{c_h-1}\left((K_1-1)^2+(K_2-1)^2+(K_3-1)^2\right)-(K_1-1)^2+\frac{2}{c_h}(K_3-1)^2} \\ &\ll K_1^2 2^{\left(\left(1+\frac{2}{c_h}\right)\frac{3}{c_h-1}-1+\frac{2}{c_h}\right)(K_1-1)^2} \\ &\ll K_1^2 2^{\left(-1+\frac{6}{c_h-1}\right)(K_1-1)^2-2K_1}, \end{aligned}$$

since $c_h > 4$. Finally

$$\begin{aligned} \int_1^2 |E_8(\alpha, K)|\,\mathrm{d}\alpha &\ll \sum_{K_4\leq K_3\leq K_2\leq K} K^2 2^{\left(-1+\frac{6}{c_h-1}\right)(K-1)^2-2K} \\ &\ll K^5 2^{\left(\frac{6}{c_h-1}-1\right)(K-1)^2-2K}, \end{aligned}$$

as claimed. $\square$

Chapter 2

Sets free of sumsets with summands of prescribed size

2.1. Introduction

A popular topic in combinatorial/additive number theory is the study of extremal sets of integers free of subsets with some given particular shape. We tackle here extremal problems about sets that do not contain sumsets with summands of prescribed size, and we show their relationship with extremal problems on graphs that are free of complete r-partite subgraphs.

Definition 2.1. *Let $r, \ell_1, \dots, \ell_r$ be integers with $r \geq 1$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$. Given an abelian group G we say that $A \subset G$ is a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set if A does not contain any sumset of the form*

$$L_1 + \cdots + L_r = \{\lambda_1 + \cdots + \lambda_r : \ \lambda_i \in L_i, \ i = 1, \dots, r\},$$

with $|L_i| = \ell_i, \ i = 1, \dots, r$. For $r = 2$ we simply write $\mathcal{L}_{\ell_1,\ell_2}$.

The degenerate case $r = 1$, that we denote by $\mathcal{L}_{\ell_1}$, is trivial: a set A is $\mathcal{L}_{\ell_1}$-free $\iff$ $|A| \leq \ell_1 - 1$.

2.1.1. $\mathcal{L}$-free sets in intervals and finite abelian groups

To motivate Definition 2.1 and the results in this work we start by summarizing the state of knowledge for some particular cases already studied in the literature.

i) $\mathcal{L}_{2,2}$*-free sets.* They are just the Sidon sets, those having the property that all the differences $a-a'$ $(a, a' \in A,\ a \neq a')$ are distinct. Indeed take $L_1 = \{a_1, b_1\},\ L_2 = \{a_2, b_2\},\ (a_i < b_i)$, then the shape of the sumset $L_1 + L_2$ can be depicted as one 2-point set plus one of its translates:

A Sidon set can be characterized as being free of this shape.

ii) $\mathcal{L}_{2,\ell}$*-free sets.* A $\mathcal{L}_{2,\ell}$-free set A is characterized by the property that there are no more than $\ell - 1$ different ways to express any non-zero element in the ambient group as a difference of two elements of A. They have been called $B_2^{\circ}[\ell - 1]$ sets [32] and $B_2^{-}[\ell - 1]$ sets [45].

For example the typical shape of a sumset $L_1 + L_2$ with $|L_1| = 2$ and $|L_2| = 3$ is one 2-point set plus two translates of it:

The $\mathcal{L}_{2,3}$-free sets are characterized as being free of this shape.

iii) $\mathcal{L}_{\ell_1,\ell_2}$*-free sets.* The sets that are free of ℓ_1 translations of sets with ℓ_2 elements were introduced by Erdős and Harzheim [18] and have been further studied in [40]. For example the $\mathcal{L}_{3,4}$-free sets are characterized by avoiding the following shape:

iv) $\mathcal{L}^{(r)}_{2,\dots,2}$*-free sets.* A Hilbert cube of dimension r is a sumset of the form $L_1+\cdots+L_r$ with $|L_1|=\cdots=|L_r|=2$. Thus $\mathcal{L}^{(r)}_{2,\dots,2}$-free sets are those free of Hilbert cubes of dimension r. A Hilbert cube of dimension 3 has this shape:

Estimating the largest size of a set $A\subset\{1,\dots,n\}$ that is $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free is an interesting and significant problem.

Definition 2.2. *We will denote by* $F\big(n,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}\big)$ *the size of a largest* $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$*-free set in the interval* $\{1,\dots,n\}$*.*

Our first result is a general upper bound that recovers known upper bounds for the particular cases considered above.

Theorem 2.1. *For any* $r\ge 2$ *and* $2\le\ell_1\le\cdots\le\ell_r$ *we have*

$$F\big(n,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}\big)\le(\ell_r-1)^{\frac{1}{\ell_1\cdots\ell_{r-1}}}n^{1-\frac{1}{\ell_1\cdots\ell_{r-1}}}+O\left(n^{\frac{1}{2}+\frac{1}{2\ell_{r-1}}-\frac{1}{\ell_1\cdots\ell_{r-1}}}\right).$$

Let us compare Theorem 2.1 with the know upper bounds for the aforementioned cases:

i) $\mathcal{L}_{2,2}$*-free sets.* The upper bound $|A|\le\sqrt{n}+O(n^{1/4})$ for any Sidon set $A\subset\{1,\dots,n\}$ was proved by Erdős and Turán [22] and refined until $|A|<\sqrt{n}+n^{1/4}+1/2$ by other authors [33, 41, 10]. The Erdős-Turán bound follows from Theorem 2.1 for $r=\ell_1=\ell_2=2$.

ii) $\mathcal{L}_{2,\ell}$*-free sets.* The upper bound $|A|<\sqrt{(\ell-1)n}+((\ell-1)n)^{1/4}+1/2$ for $B_2^\circ[\ell-1]$ sets $A\subset\{1,\dots,n\}$ was proved in [10]. Theorem 2.1 for $r=\ell_1=2$ and $\ell_2=\ell\ge 2$ gives

$$F(n,\mathcal{L}_{2,\ell})\le(\ell-1)^{1/2}n^{1/2}+O(n^{\frac{1}{4}}).$$

iii) $\mathcal{L}_{\ell_1,\ell_2}$*-free sets.* Peng, Tesoro and Timmons [40] proved that if $A \subset \{1,\dots,n\}$ does not contain ℓ_1 copies of any set of ℓ_2 elements then $|A| \le (\ell_2-1)^{1/\ell_1} n^{1-1/\ell_1} + O\left(n^{1/2-1/(2\ell_1)}\right)$. This also follows from Theorem 2.1 for $r=2$. Note that Erdős and Harzheim [18] had previously proved the weaker estimate $|A| \ll n^{1-1/\ell_1}$ for these sets.

iv) $\mathcal{L}^{(r)}_{2,\dots,2}$*-free sets.* Csaba Sándor [43] proved that if $A \subset \{1,\dots,n\}$ does not contain a Hilbert cube of dimension r then $|A| \le n^{1-1/2^{r-1}} + 2n^{1-1/2^{r-2}}$, except for finitely many n. Gunderson and Rödl [27] had previously established the weaker upper bound $|A| \ll n^{1-1/2^{r-1}}$. Theorem 2.1 in the case $\mathcal{L}^{(r)}_{2,\dots,2}$ implies

$$F(n,\mathcal{L}^{(r)}_{2,\dots,2}) \le n^{1-1/2^{r-1}} + O\left(n^{3/4-1/2^{r-1}}\right),$$

which improves the error term for $r \ge 4$ in Sándor's estimate.

The probabilistic method provides a general lower bound for $F(n,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r})$.

Theorem 2.2. *For any $r \ge 2$ and $2 \le \ell_1 \le \cdots \le \ell_r$ we have*

$$F(n,\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}) \ge n^{1-\frac{\ell_1+\cdots+\ell_r\ -r}{\ell_1\cdots\ell_r\ -1}-o(1)}.$$

The exponents in Theorems 2.1 and 2.2 are distinct and to close the gap between them is a major problem. We think that the exponent for these extremal sets is the one attained in the upper bound.

Conjecture 2.1. *For any $r \ge 2$ and $2 \le \ell_1 \le \cdots \le \ell_r$, we have*

$$F(n,\mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r}) \asymp n^{1-1/(\ell_1\cdots\ell_{r-1})}.$$

This conjecture has been proved for some particular cases:

$$F(n,\mathcal{L}_{2,\ell_2}) \sim (\ell_2-1)^{1/2} n^{1-1/2}, \tag{2.1}$$

$$F(n,\mathcal{L}_{3,\ell_2}) \asymp n^{1-1/3}, \quad (\ell_2 \ge 3), \tag{2.2}$$

$$F(n,\mathcal{L}_{\ell_1,\ell_2}) \asymp n^{1-1/\ell_1}, \quad (\ell_2 \ge (\ell_1-1)!+1). \tag{2.3}$$

The asymptotic estimate (2.1) for $\ell_2 = 2$ recovers the estimate found by Erdős and Turán [22] for extremal Sidon sets and was generalized to any $\ell_2 \ge 2$ by Trujillo-Solarte, García-Pulgarín and Velásquez-Soto [45].

The estimate (2.2) is a consequence of the following result [40]:

Theorem 2.3. *For any integer $n \geq 1$, there is a $\mathcal{L}_{3,3}$-free set $A \subset \{1, \ldots, n\}$ with*

$$|A| \geq \left(4^{-2/3} + o(1)\right) n^{2/3}.$$

The following result [40] implies the estimate (2.3):

Theorem 2.4. *Let $\ell \geq 2$ be an integer. For any integer $n \geq 1$, there is a $\mathcal{L}_{\ell,\ell!+1}$-free set $A \subset [n]$ with*

$$|A| = (1 + o(1)) \left(\frac{n}{2^{\ell-1}}\right)^{1-1/\ell}.$$

The lower bound in Theorem 2.2 has also been improved in other cases although they do not match the exponent $1-1/(\ell_1 \ldots \ell_{r-1})$. Trivially $F(n, \mathcal{L}_{4,\ell_2}) \geq F(n, \mathcal{L}_{3,\ell_2})$, thus (2.2) implies $F(n, \mathcal{L}_{4,\ell_2}) \gg n^{1-1/3}$ for $\ell_2 \geq 3$, which gives a better lower bound than Theorem 2.2 for $\ell_2 = 4, 5, 6$.

Another interesting case corresponds to $\mathcal{L}^{(3)}_{2,2,2}$-free sets. Theorem 2.2 gives the lower bound $F(n, \mathcal{L}^{(3)}_{2,2,2}) \gg n^{1-3/7-o(1)}$ but Katz, Krop and Maggioni [29] found a construction which gives

$$F(n, \mathcal{L}^{(3)}_{2,2,2}) \gg n^{1-1/3}. \tag{2.4}$$

We confirm this last lower bound with an alternative construction based upon a $\mathcal{L}^{(3)}_{2,2,2}$-free set in $\mathbb{Z}^3_{p-1}$.

Definition 2.3. *Given a finite abelian group G, we will denote by $F(G, \mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r})$ the largest size of a $\mathcal{L}^{(r)}_{\ell_1,\cdots,\ell_r}$-free set in G.*

Theorem 2.5. *For any prime $p \geq 2$ we have*

$$F(\mathbb{Z}^3_{p-1}, \mathcal{L}^{(3)}_{2,2,2}) \geq (p-3)^2.$$

The set we construct to prove Theorem 2.5 can be easily projected to the integers to prove (2.4), as it was done in [29]. In general we have

Proposition 2.1. *For any $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$, and for any $k \geq 1$ and $n_1, \ldots, n_k$, we have*

$$F(2^{k-1} n_1 \cdots n_k, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}) \geq F(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}).$$

2.1.2. Extremal problems in graphs and hypergraphs

Given a graph $\mathcal{H}$, let $\mathrm{ex}(n,\mathcal{H})$ denote the maximum number of edges (or hyperedges) of a n vertices graph (or hypergraph) which does not contain $\mathcal{H}$ as a sub-graph (or sub-hypergraph). Estimating $\mathrm{ex}(n,\mathcal{H})$ is a major problem in extremal graph theory. An important case is when $\mathcal{H}=K_{\ell_1,\ell_2}$. It is known that

$$n^{2-\frac{\ell_1+\ell_2-2}{\ell_1\ell_2-1}} \ll \mathrm{ex}(n,K_{\ell_1,\ell_2}) \le \frac{1}{2}(\ell_2-1)^{1/\ell_1} n^{2-\frac{1}{\ell_1}}(1+o(1)). \tag{2.5}$$

The upper bound was obtained by Kövari, Sós and Turán [31] and the lower bound can be easily obtained using the probabilistic method.

There is a gap between the exponents in (2.5) and to improve the exponent on the lower bound is a difficult problem. The conjecture is that the true exponent is the one attained in the upper bound. The only cases where the upper bound has been reached by a construction of a graph with $\Omega(n^{2-1/\ell_1})$ edges are

$$\mathrm{ex}(n,K_{2,2}) = \frac{1}{2}n^{3/2}(1+o(1)), \tag{2.6}$$

$$\mathrm{ex}(n,K_{2,\ell_2}) = \frac{\sqrt{\ell_2-1}}{2}n^{3/2}(1+o(1)), \quad (\ell_2\ge 2), \tag{2.7}$$

$$\mathrm{ex}(n,K_{3,3}) = \frac{1}{2}n^{5/3}(1+o(1)), \tag{2.8}$$

$$\mathrm{ex}(n,K_{\ell_1,\ell_2}) \asymp n^{2-1/\ell_1}, \quad (\ell_2 \ge (\ell_1-1)!+1). \tag{2.9}$$

Erdős, Rényi and Sós [20], and Brown [7] proved (2.6). Füredi [23] obtained (2.7) and Brown [7] and Füredi [23] proved (2.8), whereas (2.9) was proved by Alon, Rónyai and Szabó [2]. Ball and Pepe [4] have recently proved that $\mathrm{ex}(n,K_{5,5}) \gg n^{7/4}$. Their result also improves the exponent in the lower bound in (2.5) for the cases $(\ell_1,\ell_2)=(5,\ell_2),\ 5\le\ell_2\le 12$ and for $(\ell_1,\ell_2)=(6,\ell_2),\ 6\le\ell_2\le 8$.

The analogous problem for hypergraphs seems to be more difficult.

Definition 2.4. *Let $r\ge 2$ and $2\le \ell_1\le\cdots\le\ell_r$ be integers. We write $K^{(r)}_{\ell_1,\dots,\ell_r}$ for the r-uniform hypergraph $(V,\mathcal{E})$ where $V=V_1\cup\cdots\cup V_r$ with $|V_i|=\ell_i,\ i=1,\dots,r$ and*

$$\mathcal{E}=\left\{\{x_1,\dots,x_r\}:\ x_i\in V_i,\ i=1,\dots,r\right\}.$$

We will say that the r-hypergraph $\mathcal{H}$ is $K^{(r)}_{\ell_1,\dots,\ell_r}$-free when $\mathcal{H}$ does not contain any r-uniform hypergraph $K^{(r)}_{\ell_1,\dots,\ell_r}$.

We recall that $\mathrm{ex}(n; K^{(r)}_{\ell_1,\cdots,\ell_r})$ is the maximum number of hyperedges of a $K^{(r)}_{\ell_1,\dots,\ell_r}$-free hypergraph of n vertices. See [24] for a nice survey on extremal problems on graphs and hypergraphs. An easy probabilistic argument gives a lower bound which generalizes (2.5):

$$n^{r-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}} \ll \mathrm{ex}(n; K^{(r)}_{\ell_1,\cdots,\ell_r}). \tag{2.10}$$

The upper bound was considered by Erdős in the case $\ell = \ell_1 = \cdots = \ell_r$. He proved [17, Theorem 1] that

$$ex(n, K^{(r)}_{\ell,\dots,\ell}) \ll n^{r-1/\ell^{r-1}}. \tag{2.11}$$

Erdős and Simonovits wrote in [21] that probably $\lim_{n\to\infty} \frac{\mathrm{ex}(n,K^{(r)}_{\ell,\cdots,\ell})}{n^{r-1/\ell^{r-1}}}$ exists and it is a positive number. We refine the estimate (2.11) as follows.

Theorem 2.6. *For any $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ we have*

$$ex(n, K^{(r)}_{\ell_1,\dots,\ell_r}) \leq \frac{(\ell_r-1)^{1/\ell_1\cdots\ell_{r-1}}}{r!}\, n^{r-1/\ell_1\cdots\ell_{r-1}}(1+o(1)), \quad (n\to\infty). \tag{2.12}$$

The case $r = 2$ in Theorem 2.6 is the result (2.5) proved by Kövari, Sós and Turán [31]. It is believed that the upper bound in (2.12) is not far from the real value of $ex(n, K^{(r)}_{\ell_1,\dots,\ell_r})$.

Conjecture 2.2.

$$ex(n, K^{(r)}_{\ell_1,\cdots,\ell_r}) \asymp n^{r-1/\ell_1\cdots\ell_{r-1}}.$$

The lower bound in (2.10) has been improved in a few cases for $r \geq 3$:

$$\mathrm{ex}(n, K^{(3)}_{2,2,2}) \gg n^{3-1/3}, \tag{2.13}$$

$$\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) \gg n^{r-\frac{r}{2^r-1}+\frac{1}{s(2^r-1)}}, \quad (sr \equiv 1 \pmod{2^r-1}). \tag{2.14}$$

Katz, Krop and Maggioni [29] attained (2.13) and Gunderson and Rödl [27] proved (2.14). An alternative proof of (2.13) follows from Theorem 2.5 and Proposition 2.2 below.

2.1.3. Connection with extremal problems in hypergraphs

The two exponents of n in Theorems 2.1 and 2.2 have the same flavour as the two exponents of n in (2.10) and in Theorem 2.6. This is a consequence of the following result.

Proposition 2.2. *Let G be a finite abelian group with $|G| = n$. Then*

$$ex(n, K^{(r)}_{\ell_1,\dots,\ell_r}) \geq \binom{n}{r} \frac{F(G, \mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r})}{n}.$$

The proof uses $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sets in finite abelian groups to construct $K^{(r)}_{\ell_1,\dots,\ell_r}$-free hypergraphs. Proposition 2.2 connects results on extremal problems in abelian groups with results on extremal problems in hypergraphs.

We mention a couple of cases already discussed in the literature. It is well known that if A is a Sidon set in a finite abelian group G then the graph $\mathcal{G}(V, \mathcal{E})$ where $V = G$ and $\mathcal{E} = \{\{x, y\} : \ x + y \in A\}$ is a $K_{2,2}$-free graph. Another related example is the connection that was discussed in [40] between $\mathcal{L}_{\ell_1,\ell_2}$-free sets and the problem of Zarankiewicz, which in turn is connected to extremal problems on K_{ℓ_1,ℓ_2}-free graphs (see [23, §2]). As a final example (2.13) can be obtained from Theorem 2.5 by using Proposition 2.2.

In the same line of reasoning since any $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set in $\mathbb{Z}_n$ is also a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set in $\{1, \dots, n\}$ then Conjecture 2.1 implies Conjecture 2.2. The converse is not true but the algebraic ideas behind the constructions of some K_{ℓ_1,ℓ_2}-free graphs can be used in some cases to construct $\mathcal{L}_{\ell_1,\ell_2}$-free sets. This was the strategy followed in [40] to construct dense $\mathcal{L}_{3,3}$-free sets.

2.1.4. Connection with extremal problems in matrices

We denote a d-dimensional $n_1 \times \cdots \times n_d$ matrix by $A = (a_{i_1,\dots,i_d})$, where $(1 \leq i_\ell \leq n_\ell,\ 1 \leq \ell \leq d)$. Matrix A is called a 0-1 matrix if all its entries are either 0 or 1.

We will say that a d-dimensional 0-1 matrix A *contains* another 0-1 matrix

P if A has a sub-matrix that can be transformed into P by changing any number of ones to zeros. Otherwise we will say that A *avoids* P.

Definition 2.5. *Let d and n be any positive integers, and let P be a given d-dimensional matrix. We will denote by $f(n,P,d)$ the maximum number of ones in a d-dimensional $n \times \cdots \times n$ zero-one matrix that avoids a given P.*

A d-dimensional $n_1 \times \cdots \times n_d$ 0-1 matrix can be identified with a d-uniform hyper-graph (and vice versa).

Definition 2.6.

1. *Let A be a given d-dimensional $n_1 \times \cdots \times n_d$ 0-1 matrix. Let us denote by $\mathcal{G}(A) := (V, \mathcal{E})$ the hyper-graph of $n_1 + \cdots + n_d$ vertices $V = \bigcup_{1\le \ell \le d} V_\ell$, with $V_\ell = \{1, 2, \ldots, n_\ell\}$ and hyper-edges $\mathcal{E} = \{\{i_1, \ldots, i_d\} \colon a_{i_1,\ldots,i_d} = 1\}$.*
2. *Let $G = (V, \mathcal{E})$ be a d-uniform hyper-graph with $V = \bigcup_{1\le \ell \le d} V_\ell$, with $|V_\ell| = n_\ell$. Let us denote by $\mathcal{M}(G)$ the d-dimensional $n_1 \times \cdots \times n_d$ 0-1 matrix with $a_{i_1,\ldots,i_d} = 1$ if and only if $\{i_1, \ldots, i_\ell\} \in \mathcal{E}$, where $A = \mathcal{M}(G)$.*

Note that $\mathcal{G}(A)$ has as many hyper-edges as ones has the matrix A. This identification immediately brings a first connection between extremal problems in hypergraphs and extremal problems in matrices.

Proposition 2.3. *Given a hypergraph $\mathcal{H}$, let $ex(n, \mathcal{H})$ denote the maximum number of hyperedges of a n vertices hypergraph which does not contain $\mathcal{H}$ as a sub-hypergraph. Recall also definitions 2.5 and 2.6.*

Let P be any given 0-1 matrix. Then we have

$$f(n, P, d) = ex(dn, \mathcal{G}(P)). \tag{2.15}$$

Let $R^{k_1,\ldots,k_d}$ denote the d-dimensional $k_1 \times \cdots \times k_d$ matrix of all ones. Estimating $f(n, R^{k_1,k_2}, 2)$ is known as the Zarankiewicz problem. It is easy to check that the graph corresponding to R^{k_1,k_2} is the complete bipartite K_{k_1,k_2} and as a consequence we have for $f(n, R^{k_1,k_2}, 2)$ the same upper and lower bounds as in (2.5).

In the general case Geneson and Tian [25, Theorem 2.2] proved that

$$f(n, R^{k_1,\dots,k_d}, d) = O(n^{d-\alpha(k_1,\dots,k_d)}), \qquad \text{where } \alpha = \frac{\max(k_1,\dots,k_d)}{k_1k_2\cdots k_d}. \tag{2.16}$$

Using Theorem 2.6 and Proposition 2.3 we refine the estimate (2.16) as follows

Corollary 2.1. *Let $2 \le k_1 \le k_2 \le \cdots \le k_d$. Then we have*

$$f(n, R^{k_1,\dots,k_d}, d) \le \frac{(k_d-1)^\alpha d^{d-\alpha}}{d!}\, n^{d-\alpha}(1+o(1)), \quad \textit{where } \alpha = \frac{1}{k_1k_2\cdots k_{d-1}}.$$

With regards to lower bounds, the estimate (2.10) and the estimate attained by Geneson and Tian [25, Theorem 2.1] are essentially the same, in both cases obtained by the probabilistic method.

2.1.5. Extremal problems in infinite sequences of integers

We consider also infinite $\mathcal{L}$-free sequences of positive integers. This problem is more difficult than the analogous finite problem, even in the simplest case of $\mathcal{L}_{2,2}$-free sets (Sidon sequences). Let $A(x) = |A \cap [1,x]|$ be the counting function of any sequence A. In the light of Conjecture 2.1 for the finite case and being optimistic one could believe in the existence of an infinite $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sequence satisfying $A(x) \gg x^{1-1/(\ell_1\cdots\ell_{r-1})}$. Erdős [44] proved that it is not true for Sidon sequences, and Peng, Tesoro and Timmons [40] proved that neither for $\mathcal{L}_{\ell_1,\ell_2}$-free sequences this is true. We generalize these results for all $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$.

Theorem 2.7. *If A is an infinite $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sequence then*

$$\liminf_{x\to\infty} \frac{A(x)}{x}(x\log x)^{1/(\ell_1\cdots\ell_{r-1})} \ll 1.$$

Hence a natural question is *whether or not for any $\epsilon > 0$ there exists a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sequence with*

$$A(x) \gg x^{1-1/(\ell_1\cdots\ell_{r-1})-\epsilon}. \tag{2.17}$$

A positive answer to this question was conjectured by Erdős in the case of Sidon sequences. The greedy algorithm provides a Sidon sequence A with $A(x) \gg x^{1/3}$. This was the densest infinite Sidon sequence known during nearly 50 years. Ajtai, Komlós and Szemerédi [1] proved the existence of a Sidon sequence with $A(x) \gg (x \log x)^{1/3}$ and Ruzsa [42] proved the existence of a Sidon sequence with $A(x) \gg x^{\sqrt{2}-1+o(1)}$. Cilleruelo [8] constructed an explicit Sidon sequence with similar counting function.

To attain the exponent in (2.17) looks like a difficult problem. It even seems difficult to get a exponent greater than $1 - \frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}$, which is the exponent obtained in Theorem 2.2 for finite sets.

The probabilistic method used in Theorem 2.2 to construct dense finite $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free sets might be adapted to construct infinite $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free sequences with large counting function in order to prove that for every $\epsilon > 0$ there exist an infinite $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free sequence A satisfying

$$A(x) \gg x^{1-\gamma-\epsilon}, \text{ with } \gamma = \frac{\ell_1 + \cdots + \ell_r - r}{\ell_1 \cdots \ell_r - 1}.$$

We have not found a proof for the general case, however we have succeeded in two particular cases.

Theorem 2.8. *For any $\ell \geq 2$ and for any $\epsilon > 0$ there exists an infinite $\mathcal{L}_{2,\ell}$-free sequence with*

$$A(x) \gg x^{1-\frac{\ell}{2\ell-1}-\epsilon}.$$

Note however that the constructions in [42] and [8] provide a greater exponent for $\ell = 2$ and $\ell = 3$.

Theorem 2.9. *For any $r \geq 2$ and for any $\epsilon > 0$ there exists an infinite $\mathcal{L}^{(r)}_{2,\ldots,2}$-free sequence with*

$$A(x) \gg x^{1-\frac{r}{2^r-1}-\epsilon}.$$

The rest of this chapter is organized as follows. Several auxiliary results that will be used in the sequel are included in section 2.2. In section 2.3 we discuss finite sets that are $\mathcal{L}$-free and we prove Theorems 2.1, 2.2, 2.5, and Proposition 2.1. In section 2.4 firstly we prove Proposition 2.2 and Theorem 2.6 and secondly we prove Proposition 2.3 and Corollary 2.1. In section 2.5 we discuss infinite $\mathcal{L}$-free sequences of integers and prove Theorems 2.7, 2.8 and 2.9.

2.2. Lemmata and auxiliary theorems.

Lemma 2.1. *Let $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ be given. If A is a $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free set in an abelian group G then the set*

$$(A + x_1) \cap \cdots \cap (A + x_{\ell_1})$$

is a $\mathcal{L}^{(r-1)}_{\ell_2,\dots,\ell_r}$-free set for any collection $\{x_1, \dots, x_{\ell_1}\}$ of ℓ_1 distinct elements of G.

Proof. If $L_2 + \cdots + L_r \subset (A + x_1) \cap \cdots \cap (A + x_{\ell_1})$ then $L_2 + \cdots + L_r - x_i \subset A$ for $i = 1, \dots, \ell_1$ and so $L_1 + L_2 + \cdots + L_r \subset A$ for $L_1 = \{-x_1, \dots, -x_{\ell_1}\}$. □

Definition 2.7. *We say that a sumset $L_1 + \cdots + L_r$ is* degenerate *if $|L_1 + \cdots + L_r| < |L_1| \cdots |L_r|$, that is to say some of all the possible sums are repeated.*

Lemma 2.2. *If a sumset is degenerate then it contains an arithmetic progression.*

Proof. Consider the sumset $X = L_1 + \cdots + L_r$ Suppose that $x_1 + \cdots + x_r = y_1 + \cdots + y_r$ with $x_i, y_i \in L_i$ $(1 \leq i \leq r)$, and with $x_k \neq y_k$, say $x_k > y_k$, for some k. Then the three following elements of X form an arithmetic progression of difference $x_k - y_k$:

$$x_1 + \cdots + x_{k-1} + y_k + x_{k+1} + \cdots + x_r, \quad x_1 + \cdots + x_r, \quad y_1 + \cdots + y_{k-1} + x_k + y_{k+1} + \cdots + y_r.$$

□

Lemma 2.3. *Given $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$, there are at most $n^{\ell_1 + \cdots + \ell_r - r + 1}$ sumsets $X \subset \{1, \dots, n\}$ of the form $X = L_1 + \cdots + L_r$ with $|L_i| = \ell_i,\ i = 1, \dots, r$.*

Proof. Any sumset X can written in only a way in the form $x+L'_1+\cdots+L'_r$ with L'_i the translate of L_i such that $\min L'_i = 0$. The number of choices for $x, L'_1, \ldots, L'_r$ is at most $n\binom{n}{\ell_1-1}\cdots\binom{n}{\ell_r-1} < n^{1+(\ell_1-1)+\cdots+(\ell_r-1)}$. □

Lemma 2.4. *Define the map* $\varphi\colon \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}\to\mathbb{Z}$ *by*

$$\varphi(x_1,\ldots,x_k) = x_1 + x_2(2n_1) + \cdots + x_k(2n_1)(2n_2)\cdots(2n_{k-1}).$$

The map φ *is 1-to-1 and furthermore, for any* x, y, u, v *we have*

$$\varphi(x)+\varphi(y)=\varphi(u)+\varphi(v)\Rightarrow x+y=u+v. \tag{2.18}$$

Proof. We remind that *given* $r_1,\cdots,r_j,\cdots$ *(the base), any non negative integer can be written in a unique way in the form*

$$y_1+y_2r_1+y_3r_1r_2+\cdots+y_jr_1r_2\cdots r_{j-1}+\cdots\ ,$$

with digits y_j *satisfying* $0\le y_j<r_j$ $(j\ge 1)$. Hence the map $\varphi\colon \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}\to\mathbb{Z}$ given by

$$\varphi(x_1,\ldots,x_k) = x_1 + x_2(2n_1) + \cdots + x_k(2n_1)(2n_2)\cdots(2n_{k-1}),$$

is injective, to see it just note $x_1,\ldots,x_k$ are the k digits of the integer $\varphi(x_1,\ldots,x_k)$ in any base starting with $\{2n_1,2n_2,\ldots,2n_{k-1},2n_k\}$. To prove (2.18) suppose $\varphi(x)+\varphi(y)=\varphi(u)+\varphi(v)$, that is to say

$$\sum_1^k (x_j+y_j)(2n_1)(2n_2)\cdots(2n_{j-1}) = \sum_1^k (u_j+v_j)(2n_1)(2n_2)\cdots(2n_{j-1}). \tag{2.19}$$

For every $j=1,\ldots,k$ we have $0\le x_j,y_j,u_j,v_j<n_j$ which implies

$$0\le x_j+y_j,u_j+v_j<2n_j.$$

The expression of an integer in the base is unique, thus by (2.19) we have $x_i+y_j=u_j+v_j$ $(1\le j\le k)$, which implies that $x+y=u+v$.

□

Lemma 2.5. *Let p be a prime and $d \geq 1$ be an integer. Define $\phi : \mathbb{F}_p^d \to \mathbb{Z}$ by*

$$\phi((x_1, \dots, x_d)) = x_1 + 2px_2 + (2p)^2 x_3 + \cdots + (2p)^{d-1} x_d.$$

where $0 \leq x_i \leq p-1$. The map ϕ is 1-to-1 and furthermore, for any $x, y, z, t \in \mathbb{F}_p^d$, we have $x + y = z + t$ if and only if $\phi(x) + \phi(y) = \phi(z) + \phi(t)$.

In the language of additive combinatorics, the map ϕ is a Frieman isomorphism of order 2.

Proof. The proof of Lemma 2.5 is easy, following the same lines of the proof of Lemma 2.4. □

We recall a Theorem, which is a consequence of the Jensen's inequality, and that will be used in the proof of Theorem 2.6.

Theorem 2.10 (Overlapping Theorem [12])**.** *Let $(\Omega, \mathcal{A}, \mathbb{P})$ be a probability space and let $\{E_j\}_{j=1}^k$ denote a family of events. Write*

$$\sigma_r := \sum_{1 \leq j_1 < \cdots < j_r \leq k} \mathbb{P}\left(E_{j_1} \cap \cdots \cap E_{j_r}\right), \quad (r \geq 1).$$

Then we have

$$\sigma_r \geq \binom{\sigma_1}{r} = \frac{\sigma_1(\sigma_1 - 1) \cdots (\sigma_1 - (r-1))}{r!}.$$

An inmediate corollary of Theorem 2.10 is the following lemma which will be used several times through this work.

Lemma 2.6. *Let $r \geq 2$ be an integer. If $A + B \subset X$ then*

$$\frac{1}{|X|} \sum_{\{x_1, \dots, x_r\} \in \binom{B}{r}} |(A + x_1) \cap \cdots \cap (A + x_r)| \geq \binom{\frac{|A||B|}{|X|}}{r}. \tag{2.20}$$

Behrend [5] proved the following result that will be used in the random constructions we make in the sequel.

Theorem 2.11 (Behrend). *For n large enough, any set of n consecutive integers contains a subset B_n free of arithmetic progressions with size $|B_n| = n^{1-\omega(n)}$, for some decreasing function $\omega(n) \to 0$ when $n \to \infty$.*

Indeed it is possible to take $\omega(n) \asymp 1/\sqrt{\log n}$.

2.3. Proofs of results for finite $\mathcal{L}$-free sets

2.3.1. Proof of Theorem 2.1

Theorem 2.1 *For any $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ we have*

$$F\big(n, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}\big) \leq (\ell_r - 1)^{\frac{1}{\ell_1\cdots\ell_{r-1}}} n^{1-\frac{1}{\ell_1\cdots\ell_{r-1}}} + O\left(n^{\frac{1}{2}+\frac{1}{2\ell_{r-1}}-\frac{1}{\ell_1\cdots\ell_{r-1}}}\right).$$

As the first step in the proof we attain a weaker version of the upper bound of Theorem 2.1.

Lemma 2.7. *For $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ we have*

$$F\big(n, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}\big) \ll n^{1-1/(\ell_1\cdots\ell_{r-1})}.$$

Proof. For short we write $F_r = F\big(n, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}\big)$ and $F_{r-1} = F\big(n, \mathcal{L}^{(r-1)}_{\ell_2,\ldots,\ell_r}\big)$. Suppose that $A \subset [n]$ is a $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free set of largest cardinality, so we have $|A| = F_r$. Lemma 2.1 implies that

$$|(A + x_1) \cap \cdots \cap (A + x_{\ell_1})| \leq F_{r-1}, \tag{2.21}$$

holds for any set of distinct positive integers $\{x_1, \ldots, x_{\ell_1}\}$.

Now we take $B = [1, n]$ and $X = [1, 2n]$ in Lemma 2.6 and use (2.21) to get

$$\frac{1}{2n}\binom{n}{\ell_1} F_{r-1} \geq \binom{F_r/2}{\ell_1} \implies \frac{n^{\ell_1-1}}{2} F_{r-1} > (F_r/2 - (\ell_1 - 1))^{\ell_1},$$

and then we have

$$F_r < (2n)^{1-1/\ell_1}(F_{r-1})^{1/\ell_1} + 2\ell_1. \tag{2.22}$$

This inequality allow us to prove Lemma 2.7 using induction on r. First note that $F_1 = F(n, \mathcal{L}_{\ell_2}) = \ell_2 - 1$ for $n \geq \ell_2 - 1$ and inserting (2.22) we have that the Lemma is true for $r = 2$.

Assume that it is true for $r-1$. Inequality (2.22) implies

$$F_r \ll n^{1-1/\ell_1}(F_{r-1})^{1/\ell_1} \ll n^{1-1/\ell_1}(n^{1-1/(\ell_2\cdots\ell_{r-1})})^{1/\ell_1} \ll n^{1-1/(\ell_1\cdots\ell_{r-1})}.$$

$\square$

Next we will prove a refined version of the inequality (2.22).

Lemma 2.8. *Let $r, \ell_1, \ldots, \ell_r$ be integers with $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$. We have the following inequality:*

$$F\big(n, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}\big) < n^{1-\frac{1}{\ell_1}}\left(F\big(n, \mathcal{L}^{(r-1)}_{\ell_2,\ldots,\ell_r}\big)\right)^{\frac{1}{\ell_1}} + O\left(n^{1/2-1/(2\ell_1\cdots\ell_{r-1})}\right).$$

Proof. The first part of the proof is similar to the proof of Lemma 2.7 but now we take $B = [0, m]$ and $X = [1, n+m]$ in Lemma 2.6 where m will be choosen later. The inequality (2.21) and Lemma 2.6 imply

$$\begin{aligned}
\frac{F_{r-1}}{n+m}\binom{m+1}{\ell_1} &\geq \binom{\frac{(m+1)F_r}{n+m}}{\ell_1} \\
\Longrightarrow \frac{F_{r-1}}{n+m}(m+1)^{\ell_1} &\geq \left(\frac{(m+1)F_r}{n+m} - (\ell_1 - 1)\right)^{\ell_1} \\
\Longrightarrow \frac{F_{r-1}}{n+m} &\geq \left(\frac{F_r}{n+m} - \frac{\ell_1 - 1}{m+1}\right)^{\ell_1} \\
\Longrightarrow \frac{F_r}{n+m} &\leq \left(\frac{F_{r-1}}{n+m}\right)^{1/\ell_1} + \frac{\ell_1 - 1}{m+1}.
\end{aligned}$$

Using that $(n+m)^{1-1/\ell_1} = n^{1-1/\ell_1}(1+m/n)^{1-1/\ell_1} < n^{1-1/\ell_1}(1+m/n)$ we get

$$\begin{aligned}
F_r &\leq (n+m)^{1-1/\ell_1}{F_{r-1}}^{1/\ell_1} + \frac{(\ell_1-1)(n+m)}{m+1} \\
&\leq n^{1-1/\ell_1}{F_{r-1}}^{1/\ell_1}\left(1 + \frac{m}{n}\right) + \frac{(\ell_1-1)(n+m)}{m+1} \\
&\leq n^{1-1/\ell_1}{F_{r-1}}^{1/\ell_1} + m\left(\frac{F_{r-1}}{n}\right)^{1/\ell_1} + \frac{(\ell_1-1)n}{m+1} + \ell_1 - 1.
\end{aligned}$$

To make as sharp as possible this last estimate we need that the second and the third summands have the same order of magnitude. Hence by taking $m = \lfloor \sqrt{n\ell_1}/(F_{r-1}/n)^{1/(2\ell_1)} \rfloor$ and using also Lemma 2.7 we have

$$(2.23) \qquad \begin{aligned} F_r &\le n\,(F_{r-1}/n)^{1/\ell_1} + 2\frac{\ell_1 - 1}{\sqrt{\ell_1}}\sqrt{n}\,(F_{r-1}/n)^{1/(2\ell_1)} + \ell_1 - 1 \\ &< n^{1-1/\ell_1} F_{r-1}^{1/\ell_1} + O\big(n^{1/2 - 1/(2\ell_1\cdots\ell_{r-1})}\big), \end{aligned}$$

as claimed. □

To finish the proof of Theorem 2.1 we proceed by induction on r. For $r = 2$, let $F_2 = F(n, \mathcal{L}_{\ell_1,\ell_2})$ and $F_1 = F(n, \mathcal{L}_{\ell_2})$. Observe that $F_1 = \ell_2 - 1$ for $n \ge \ell_2 - 1$. Inequality (2.23) implies

$$F_2 < (\ell_2 - 1)^{1/\ell_1} n^{1-1/\ell_1} + O\left(n^{1/2-1/(2\ell_1)}\right).$$

Assume that Theorem 2.1 is true for $r - 1$ and take any $\ell_1, \ldots, \ell_r$ with $2 \le \ell_1 \le \cdots \le \ell_r$. Lemma 2.8 and the induction hypothesis imply

$$\begin{aligned} F_r &< n^{1-1/\ell_1}\,(F_{r-1})^{1/\ell_1} + O\left(n^{1/2-1/(2\ell_1\cdots\ell_{r-1})}\right) \\ &< n^{1-1/\ell_1}\left((\ell_r - 1)^{\frac{1}{\ell_2\cdots\ell_{r-1}}} n^{1-\frac{1}{\ell_2\cdots\ell_{r-1}}} + O\left(n^{\frac12+\frac{1}{2\ell_{r-1}}-\frac{1}{\ell_2\cdots\ell_{r-1}}}\right)\right)^{1/\ell_1} \\ &+ O\left(n^{\frac12-\frac{1}{2\ell_1\cdots\ell_{r-1}}}\right) \\ &< (\ell_r - 1)^{\frac{1}{\ell_1\cdots\ell_{r-1}}} n^{1-\frac{1}{\ell_1\cdots\ell_{r-1}}}\left(1 + O\left(n^{-\frac12+\frac{1}{2\ell_{r-1}}}\right)\right)^{1/\ell_1} + O\left(n^{\frac12-\frac{1}{2\ell_1\cdots\ell_{r-1}}}\right) \\ &< (\ell_r - 1)^{\frac{1}{\ell_1\cdots\ell_{r-1}}} n^{1-\frac{1}{\ell_1\cdots\ell_{r-1}}} + O\left(n^{\frac12+\frac{1}{2\ell_{r-1}}-\frac{1}{\ell_1\cdots\ell_{r-1}}}\right) + O\left(n^{\frac12-\frac{1}{2\ell_1\cdots\ell_{r-1}}}\right) \end{aligned}$$

For $r = 2$ the second and third summands are the same. For $r > 2$ note that $\ell_1 \cdots \ell_{r-2} - 2 > -1$, and dividing this inequality by $2\ell_1 \cdots \ell_{r-1}$ we have that the exponent in the third summand is smaller than the exponent in the second summand. Hence we have

$$F_r < (\ell_r - 1)^{\frac{1}{\ell_1\cdots\ell_{r-1}}} n^{1-\frac{1}{\ell_1\cdots\ell_{r-1}}} + O\left(n^{\frac12+\frac{1}{2\ell_{r-1}}-\frac{1}{\ell_1\cdots\ell_{r-1}}}\right),$$

as claimed.

2.3.2. Proof of Theorem 2.2

Theorem 2.2 *For any $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ we have*

$$F(n, \mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}) \geq n^{1-\frac{\ell_1+\cdots+\ell_r \ -r}{\ell_1\cdots\ell_r \ -1}-o(1)}.$$

The lower bound of Theorem 2.2 comes from a probabilistic construction. Our proof is a generalization of the argument that Gunderson and Rodl [27] used for the particular case $\mathcal{L}^{(r)}_{2,\dots,2}$.

Let B_n denote the set given by Theorem 2.11 of Behrend, with the following properties: $B_n \subset [n]$, B is free of arithmetic progressions and its size is $|B_n| = n^{1-\omega(n)}$. with $\omega(n) = o(1)$.

Next we randomly construct a set S in $[n]$ with the following probability law:

$$\mathbb{P}(\nu \in S) = \begin{cases} p \text{ if } \nu \in B_n, \\ 0 \text{ otherwise,} \end{cases}$$

where all the events $\{\nu \in S\}_{\nu \geq 1}$ are mutually independent. For the value of p we choose

$$p = p(n) = \frac{1}{2} n^{\frac{r-(\ell_1+\cdots+\ell_r)-\omega(n)}{\ell_1\cdots\ell_r-1}}.$$

We will say that X is an *obstruction* (for S) when $X \subset S$ is a sumset of the class $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$. Our aim is to destroy all the obstructions for S. To this end we will remove from S the greatest element of every obstruction. Let S^{bad} denote the collection of all these greatest elements:

$$S^{\mathrm{bad}} := \bigcup_{\substack{X \subset S \\ X \in \mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}}} \{\max(X)\}. \tag{2.24}$$

If the number of obstructions is low enough, then we could remove from S all the elements in the collection S^{bad} and still retain a sufficiently dense set which would be free of obstructions. With this in mind we claim that the obstructions for S are few in our construction.

Lemma 2.9. *For all n sufficiently large, with probability at least $1/4$ the random sets constructed in this way satisfy*

$$|S| \geq \frac{|B_n|p}{2} \quad \textit{and} \quad |S^{\mathrm{bad}}| \leq \frac{|B_n|p}{4}.$$

The lemma implies that there exist a set $S \subset [n]$ such that

$$|S \setminus S^{\mathrm{bad}}| > \frac{|B_n|p}{4} = n^{1-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}-o(1)}.$$

Note that the set $A = S\setminus S^{\mathrm{bad}}$ satisfies the conditions of Theorem 2.2. Indeed by removing from S all the elements in S^{bad} we have that A is $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free because all the sumsets of the class $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$ that were contained in S have been destroyed.

Thus to complete the proof of Theorem 2.2 all we need is to prove Lemma 2.9.

Proof of Lemma 2.9. On the one hand since $S \subset B_n$, then S is free of arithmetic progressions and Lemma 2.2 implies that all the obstructions for S are non-degenerate (see definition 2.7). Hence all the possible sums within an obstruction X are distinct and so the probability of any obstruction X to occur in the construction is

$$\mathbb{P}(X \subset S \colon X \in \mathcal{L}^{(r)}_{\ell_1,\ldots\ell_r}) = p^{\ell_1\cdots\ell_r}. \tag{2.25}$$

Consider the random variable $N(S) = \#\{X \subset S \colon X \in \mathcal{L}^{(r)}_{\ell_1,\ldots\ell_r}\}$ that counts the number of obstructions. As two different obstructions may have the same maximum then $N(S)$ is greater or equal than the cardinality of S^{bad}. Hence using Lemma 2.3 and (2.25) we can estimate the expected cardinal of S^{bad} as follows:

$$\begin{aligned}
\mathbb{E}\left(|S^{\mathrm{bad}}|\right) &\leq \mathbb{E}(N(S)) = \#\{X \subset [n] : \ X \in \mathcal{L}^{(r)}_{\ell_1,\ldots\ell_r}\}\ \mathbb{P}(X \subset S) \\
&\leq n^{\ell_1+\cdots+\ell_r-r+1}p^{\ell_1\cdots\ell_r} \\
&= 2^{-\ell_1\cdots\ell_r}n^{\ell_1+\cdots+\ell_r-r+1}n^{\frac{r-(\ell_1+\cdots+\ell_r)-\omega(n)}{\ell_1\cdots\ell_r-1}(\ell_1\cdots\ell_r-1+1)} \\
&= 2^{-\ell_1\cdots\ell_r}n^{1-\omega(n)}n^{\frac{r-(\ell_1+\cdots+\ell_r)-\omega(n)}{\ell_1\cdots\ell_r-1}} = |B_n|p/2^{\ell_1\cdots\ell_r-1}.
\end{aligned}$$

Using the fact that $2 \leq \ell_i$ $(2 \leq i \leq r)$, this last estimate of $\mathbb{E}(|S^{\text{bad}}|)$, and Markov inequality we have

$$\begin{aligned} \mathbb{P}\left(|S^{\text{bad}}| > \frac{|B_n|p}{4}\right) &\leq \mathbb{P}\left(|S^{\text{bad}}| > \frac{|B_n|p}{2^{\ell_1\cdots\ell_r-2}}\right) \\ &\leq \mathbb{P}\left(|S^{\text{bad}}| > 2\,\mathbb{E}(|S^{\text{bad}}|)\right) \leq 1/2. \end{aligned} \tag{2.26}$$

On the other hand the size of S equals $\sum_{\nu\in B_n} 1_{\nu\in S}$, i.e: the sum of $|B_n|$ independent random indicator variables all having the same expectation p and variance $p(1-p)$. This implies $\mathbb{E}(|S|) = |B_n|p$ and $\text{Var}(|S|) = |B_n|p(1-p)$. We can now use Chebychev inequality to write

$$\begin{aligned} \mathbb{P}\left(|S| < \frac{|B_n|p}{2}\right) = \mathbb{P}\left(|S| < \frac{\mathbb{E}(|S|)}{2}\right) &< \mathbb{P}\left((|S - \mathbb{E}(|S|)| > \frac{\mathbb{E}(|S|)}{2}\right) \\ &< \frac{4\text{Var}(|S|)}{(\mathbb{E}(|S|))^2} = \frac{4|B_n|p(1-p)}{(|B_n|p)^2} < \frac{4}{|B_n|p} < \frac{1}{4}, \end{aligned} \tag{2.27}$$

except for finitely many n, since $|B_n|p \to \infty$. Combining (2.26) and (2.27) we obtain

$$\mathbb{P}\left(|S| \geq |B_n|p/2 \text{ and } |S^{\text{bad}}| \leq |B_n|p/4\right) \geq 1 - (1/2 + 1/4) \geq 1/4,$$

as claimed. □

2.3.3. Proof of Theorems 2.3 and 2.4

Theorem 2.3 *For any integer $n \geq 1$, there is a $\mathcal{L}_{3,3}$-free set $A \subset \{1, \ldots, n\}$ with*

$$|A| \geq \left(4^{-2/3} + o(1)\right) n^{2/3}.$$

Theorem 2.4 *Let $\ell \geq 2$ be an integer. For any integer $n \geq 1$, there is a $\mathcal{L}_{\ell,\ell!+1}$-free set $A \subset [n]$ with*

$$|A| = (1 + o(1)) \left(\frac{n}{2^{\ell-1}}\right)^{1-1/\ell}.$$

Theorem 2.3 is a consequence of the following result.

Theorem 2.12. *Let $p > 3$ be an odd prime and $\alpha \in \mathbb{F}_p$ be chosen to be a quadratic non-residue if $p \equiv 1 (\mathrm{mod}\ 4)$, and a nonzero quadratic residue otherwise. The set*

$$A = \{(x_1, x_2, x_3) \in \mathbb{F}_p^3 : x_1^2 + x_2^2 + x_3^2 = \alpha\}$$

is $\mathcal{L}_{3,3}$-free in the group $\mathbb{F}_p^3$, with $|A| \geq p^2 - p$.

Proof of Theorem 2.12. Recall that we choose $\alpha \in \mathbb{F}_p$ as a quadratic non-residue when $p \equiv 1(\mathrm{mod}\ 4)$ and a non-zero quadratic residue otherwise. Let $G = (V, E)$ be a graph over $\mathbb{F}_p^3$. For $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ we have $(x, y) \in E(G)$ if and only if

$$\sum_{i=1}^{3} (x_i - y_i)^2 = \alpha.$$

The graph G is $K_{3,3}$-free as shown by Brown [7]. Notice that we define

$$S(\alpha) = \{x = (x_1, x_2, x_3) \in \mathbb{F}_p^3 \colon x_1^2 + x_2^2 + x_3^2 = \alpha\}.$$

Let $X = \{x, y, z\} \subset \mathbb{F}_p^3$. Suppose $X + a \subset S(\alpha)$ for some $a \in \mathbb{F}_p^3$. We first show $-a \notin \{x, y, z\}$. Suppose $x = -a$ then we get $0 = \alpha$ as $x + a \in S(\alpha)$. However we have $\alpha \neq 0$ by the choice of α, which is a contradiction. We obtain that $(x, -a), (y, -a)$, and $(z, -a)$ are three edges in G, which tell us that x, y, and z have a common neighbour a. Assume there are three translates $X + a, X + b, X + c$ contained in $S(\alpha)$ for distinct $a, b, c \in \mathbb{F}_p^3$. We have $\{x, y, z\} \cap \{a, b, c\} = \emptyset$ and then $L = \{x, y, z\}$ and $R = \{a, b, c\}$ form a $K_{3,3}$ in G. However G is $K_{3,3}$-free. We obtain a contradiction. Thus there are at most two elements $a, b \in \mathbb{F}_p^3$ such that $X + \{a, b\}$ is contained in $S(\alpha)$. This holds for every $X \subset \mathbb{F}_p^3$ with $|X| = 3$. Then $A = S(\alpha)$ is $\mathcal{L}_{3,3}$-free. $\square$

Proof of Theorem 2.3. Let n be a large integer. Choose a prime $p > 3$ with $4p^3 \leq n$ and p as large as possible. Let $S \subset \mathbb{F}_p^3$ be a $\mathcal{L}_{3,3}$-free set in $\mathbb{F}_p^3$

with $|S| \geq p^2 - p$ guaranteed by Theorem 2.12. Consider $A = \phi(S)$ where $\phi : \mathbb{F}_p^3 \to \mathbb{Z}$ is the map

$$\phi((x_1, x_2, x_3)) = x_1 + 2px_2 + 4p^2x_3$$

Here x_i is chosen so that $0 \leq x_i \leq p - 1$. By Lemma 2.5, A is $\mathcal{L}_{3,3}$-free. If $a \in A$, then $a \leq (p-1)(1 + 2p + 4p^2) \leq 4p^3 \leq n$ so $A \subset \{1, \ldots, n\}$. Since ϕ is 1-to-1, $|A| \geq p^2 - p$. For large enough n, there is always a prime between $(n/4)^{1/3} - (n/4)^{\theta/3}$ and $(n/4)^{1/3}$ for some $\theta < 1$. The results of [6] show that one can take $\theta = 0.525$. Therefore, $|A| \geq (n/4)^{2/3} - O(n^{\frac{\theta+1}{3}}) = (1 + o(1))(n/4)^{2/3}$. □

Proof of Theorem 2.4. Let q be a prime power and $\ell \geq 2$ be an integer. Let $N : \mathbb{F}_{q^\ell} \to \mathbb{F}$ be the norm map defined by

$$N(x) = x^{1+q+q^2+\cdots+q^{\ell-1}}.$$

Let $A = \{x \in \mathbb{F}_{q^\ell} : N(x) = 1\}$. The norm map N is a group homomorphism that maps $\mathbb{F}_{q^\ell}^*$ onto $\mathbb{F}_q^*$. This implies $\frac{q^\ell-1}{|A|} = q - 1$ so $|A| = \frac{q^\ell-1}{q-1}$. We now show that A is a $\mathcal{L}_{\ell,\ell!+1}$-free set in the group $\mathbb{F}_{q^\ell}$.

Suppose $X = \{x_1, \ldots, x_\ell\} \subset \mathbb{F}_{q^\ell}$. It follows from Theorem 3.3 of [30] that there are at most $\ell!$ elements $k \in \mathbb{F}_{q^\ell}$ such that

$$N(k + x_i) = 1,$$

for all $1 \leq i \leq \ell$. Therefore, given any set $\{k_1, \ldots, k_{\ell!+1}\} \subset \mathbb{F}_{q^\ell}$, at least one of the translates $X + k_i$ is not contained in A.

Let $\psi : \mathbb{F}_{q^\ell} \to \mathbb{Z}_q^\ell$ be a group isomorphism mapping the additive group $\mathbb{F}_{q^\ell}$ onto the direct product $\mathbb{Z}_q^\ell$. Let $\phi : \mathbb{Z}_q^\ell \to \mathbb{Z}$ be the map

$$\phi(x_1, \ldots, x_\ell) = x_1 + (2q)x_2 + \cdots + (2q)^{\ell-1}x_\ell$$

where $0 \leq x_i \leq q - 1$. By Lemma 2.5, $A' := \phi(\psi(A))$ is a $\mathcal{L}_{\ell,\ell!+1}$-free set. The set A' has $\frac{q^\ell-1}{q-1}$ elements and is contained in the set $[2^{\ell-1}q^\ell]$. By the same argument as the one for proving Theorem 2.3 we can choose q properly for n large enough to obtain a $\mathcal{L}_{\ell,\ell!+1}$-free set in $\{1, \ldots, n\}$ with size $(1 + o(1))\left(\frac{n}{2^{\ell-1}}\right)^{1-1/\ell}$. □

2.3.4. Proof of Theorem 2.5

Theorem 2.5 *For any prime $p \geq 2$ we have*

$$F(\mathbb{Z}_{p-1}^3, \mathcal{L}_{2,2,2}^{(3)}) \geq (p-3)^2.$$

Theorem 2.5 is an immediate corollary of the following result.

Proposition 2.4. *Let p be an odd prime and θ be a generator of $\mathcal{F}_p^*$. The set*

$$A = \{(x_1, x_2, x_3) : \ \theta^{x_1} + \theta^{x_2} + \theta^{x_3} = 1, \ x_1, x_2, x_3 \neq 0\} \subset \mathbb{Z}_{p-1}^3$$

does not contain subsets of the form $L_1 + L_2 + L_3$ with $|L_1| = |L_2| = |L_3| = 2$ and has $(p-3)^2$ elements.

Proof. The first observation is that, given any abelian group G, a set $A \subset G$ is free of subsets of the form $L_1 + L_2 + L_3$, $|L_1| = |L_2| = |L_3| = 2$ if and only if for any $y \in G$, $y \neq 0$, the sets $A^y = A \cap (A + y)$ do not contain subsets of the form $L_1 + L_2$, $|L_1| = |L_2| = 2$. This last condition is equivalent to say that A^y is a Sidon set. This is what we have to prove.

For a fixed $y = (y_1, y_2, y_3) \neq (0, 0, 0)$ in $\mathbb{Z}_{p-1}^3$ we consider the set $A^y = A \cap (A + y)$. It is clear from the definition that

$$A^y = \{(x_1, x_2, x_3) : \text{ satisfying the conditions } (*)\}$$

$$(*) \qquad \begin{cases} \theta^{x_1} + \theta^{x_2} + \theta^{x_3} = 1 \\ \theta^{x_1+y_1} + \theta^{x_2+y_2} + \theta^{x_3+y_3} = 1 \\ x_i, x_i + y_i \neq 0, \ i = 1, 2, 3. \end{cases}$$

We claim that, if A^y is not empty, then one of the coordinates of y is distinct from 0 and distinct from the other two coordinates.

To prove this claim suppose that $(x_1, x_2, x_3) \in A^y$. Since $y = (y_1, y_2, y_3) \neq (0, 0, 0)$ we can assume that one of the coordinates is different from zero, say

$y_3 \neq 0$. If $y_3 \neq y_1$ and $y_3 \neq y_2$ then the coordinate y_3 satisfies the statement of the claim. We consider now the possibility that $y_3 = y_2$ (the case $y_3 = y_1$ is similar). We will see that in this case, the coordinate y_1 satisfies the claim. If $y_1 = 0$ then the equations (*) imply that $\theta^{x_1} + \theta^{x_2} = \theta^{y_3}(\theta^{x_1} + \theta^{x_2})$ and then, since $y_3 \neq 0$, we have that $\theta^{x_1} + \theta^{x_2} = 0$. But it implies that $x_3 = 0$ which is not possible by construction. Furthermore it is clear that $y_1 \neq y_2 = y_3$. Otherwise we would have that $y_1 = y_2 = y_3$ and the equations (*) would imply that $y = (0, 0, 0)$ which is a contradiction.

Let us assume that y_3 is distinct from 0 and distinct from the other two coordinates. This implies that the elements $\lambda_1 = \theta^{y_3} - \theta^{y_1}$, $\lambda_2 = \theta^{y_3} - \theta^{y_2}$ and $\mu = \theta^{y_3} - 1$ are distinct from zero. Hence taking the function $x_3(x_1, x_2) = \log_\theta(1 - \theta^{x_1} - \theta^{x_2})$ we can deduce from the equations in (*) that the set A^y is included in the set

$$S = \{(x_1, x_2, x_3(x_1, x_2)) : \ \lambda_1\theta^{x_1} + \lambda_2\theta^{x_2} = \mu, \ \theta^{x_1} + \theta^{x_2} \neq 1\}.$$

Next we show that S is a Sidon set, which implies that A^y is a Sidon set. For a given $(z_1, z_2, z_3) \neq (0, 0, 0)$, suppose that

$$(x_1, x_2, x_3(x_1, x_2)) - (x_1', x_2', x_3(x_1', x_2')) = (z_1, z_2, z_3) \tag{2.28}$$

with

$$\begin{cases} \lambda_1\theta^{x_1} + \lambda_2\theta^{x_2} = \mu, \\ \lambda_1\theta^{x_1'} + \lambda_2\theta^{x_2'} = \mu. \end{cases} \tag{2.29}$$

We will show that $(x_1, x_2, x_3(x_1, x_2))$ and $(x_1', x_2', x_3(x_1', x_2'))$ are uniquely determined by the conditions (2.28) and (2.29). If $z_1 = z_2 = 0$ then $(x_1, x_2) = (x_1', x_2')$, which implies that $z_3 = 0$. Therefore we can assume that $(z_1, z_2) \neq (0, 0)$. In this case equations in (2.28) and (2.29) imply that

$$\lambda_2\theta^{x_2}(1 - \theta^{z_1 - z_2}) = \mu(1 - \theta^{z_1}).$$

If $z_1 = z_2$ then $\mu(1 - \theta^{z_1}) = 0 \implies z_1 = z_2 = 0$. If $z_1 \neq z_2$ then x_2 is uniquely determined and therefore also $x_1, x_1', x_2', x_3(x_1, x_2)$ and $x_3(x_1', x_2')$.

To complete the proof of the lemma we calculate the size of A:

$$\begin{aligned}
|A| &= |\{(u,v,w)\in \mathcal{F}_p^3 : u+v+w=1,\ u,v,w\notin\{0,1\}\}| \\
&= \sum_{w\notin\{0,1\}}\ \sum_{v\notin\{0,1,-w,1-w\}} 1 = \sum_{w\notin\{0,1\}} (p-|\{0,1,-w,1-w\}|) \\
&= p(p-2) - \sum_{w\notin\{0,1,-1\}} |\{0,1,-w,1-w\}| - |\{0,1,1,2\}| \\
&= p(p-2) - 4(p-3) - 3 = (p-3)^2.
\end{aligned}$$

□

In the rest of this section we will prove the estimate (2.4) by using Theorem 2.5 and the following projection from $\mathbb{Z}_m^3$ to $\mathbb{Z}$. For any integer $m \geq 2$ we consider the function $\varphi_m : \mathbb{Z}_m^3 \to \mathbb{Z}$ defined by

$$\varphi_m(x_1,x_2,x_3) = (2m)^2x_1 + (2m)x_2 + x_3, \tag{2.30}$$

where x_1, x_2, x_3 are residues in $[0, m-1]$. An easy, but important, property of this function is that

$$\varphi_m(x)+\varphi_m(y) = \varphi_m(u)+\varphi_m(v) \implies x+y=u+v. \tag{2.31}$$

For a proof, refer to Lemmas 2.5 and 2.4.

Lemma 2.10. *If $A \subset \mathbb{Z}_m^3$ is $\mathcal{L}^{(3)}_{2,2,2}$-free then the set $\varphi_m(A)$ is $\mathcal{L}^{(3)}_{2,2,2}$-free over the integers.*

Proof. A Hilbert cube of dimension 3 can be also described as a multiset $\{x_1,\dots,x_8\}$ with $x_2, x_3, x_5 \neq x_1$ satisfying the following conditions (see the picture below):

$$\begin{cases} x_2 - x_1 = x_4 - x_3 = x_6 - x_5 = x_8 - x_7 \\ x_3 - x_1 = x_7 - x_5 \end{cases}$$

This system of equations is equivalent to the following system in term of sums:

$$\begin{cases} x_2 + x_3 = x_4 + x_1, \\ x_2 + x_5 = x_6 + x_1, \\ x_2 + x_7 = x_8 + x_1, \\ x_3 + x_5 = x_7 + x_1. \end{cases} \tag{2.32}$$

Suppose that $\{\varphi_m(a_1), \ldots, \varphi_m(a_8)\}$ with $a_1, \ldots, a_8 \in A$ is a Hilbert cube of dimension 3 contained in $\varphi_m(A)$. Since the elements $\varphi_m(a_1), \ldots, \varphi_m(a_8)$ satisfy the four equations in (2.32), the observation (2.31) implies that also the elements $a_1, \ldots, a_8$ satisfy the analogous equations in $\mathbb{Z}_m^3$ and therefore the multiset $\{a_1, \ldots, a_8\}$ is a Hilbert cube of dimension 3 contained in A. $\square$

To attain bound (2.4) we apply Lemma 2.10 to the set A described in Proposition 2.4. It is easy to see that φ_m defined by (2.30) is injective thus $|\varphi_{p-1}(A)| = |A| = (p-3)^2$ and we also have $\varphi_{p-1}(A) \subset [0, 4(p-1)^3)$. Let p be the largest prime p such that $4(p-1)^3 \le n$, that is $p = (n/4)^{1/3}(1+o(1))$. Then we have

$$F(n, \mathcal{L}^{(3)}_{2,2,2}) \ge |\varphi_{p-1}(A)| = (p-3)^2 = (n/4)^{2/3}(1+o(1)).$$

2.3.5. Proof of Proposition 2.1

Proposition 2.1 *For any $r \ge 2$ and $2 \le \ell_1 \le \cdots \le \ell_r$, and for any $k \ge 1$ and $n_1, \ldots, n_k$, we have*

$$F(2^{k-1} n_1 \cdots n_k, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}) \ge F(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}).$$

To prepare for the proof we first generalize the idea that we used during the proof of Lemma 2.10. The sums in a sumset might be repeated thus we have a multiset in the general case. However a minimum number of the sums are distinct. The set L_1 is translated ℓ_2 times to form a pattern which is in turn translated ℓ_3 times and so on. The next lemma characterizes sumsets as multisets satisfying a number of conditions.

Lemma 2.11. *Let $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ be given, and a sumset $L_1 + \cdots + L_r \in \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$, with summands $L_s = \{\lambda_{s1}, \ldots, \lambda_{s\ell_s}\}$, $(1 \leq s \leq r)$. We enumerate the sums using a multi-index as follows:*

$$x_{i_1 i_2 \cdots i_r} := \sum_{s=1}^{r} \lambda_{s i_s}, \quad (1 \leq i_s \leq \ell_s,\ 1 \leq s \leq r).$$

Then the following $\sum_{k=1}^{r} \binom{\ell_k}{2}$ conditions hold:

$$x_{1\cdots 1 i_s 1 \cdots 1} \neq x_{1\cdots 1 j_s 1\cdots 1}, \quad (1 \leq i_s < j_s \leq \ell_s, s = 1, \ldots, r). \tag{2.33}$$

Furthermore the following $\ell_1 \cdots \ell_r - (\ell_1 + \cdots + \ell_r) + (r-1)$ equalities hold:

$$x_{1\cdots 1} + x_{1\cdots 1 i_s i_{s+1} \cdots i_r} = x_{1\cdots 1 i_s 1 \cdots 1} + x_{1\cdots 1 i_{s+1}\cdots i_r}, \quad \big(i_s \neq 1,\ (i_{s+1}, \ldots, i_r) \neq (1, \ldots, 1), 1 \leq s < r\big). \tag{2.34}$$

In the other direction, suppose that a given multiset X of $\ell_1 \cdots \ell_r$ elements can be multi-indexed as follows

$$X = \{x_{i_1 \cdots i_r}, \quad 1 \leq i_s \leq \ell_s, 1 \leq s \leq r\},$$

so that conditions (2.33) *and* (2.34) *are satisfied. Then $X \in \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$.*

Proof. For $s = 1, \ldots, r$ the cardinality of any translate of L_s is ℓ_s. Hence all the elements in the translate

$$\sum_{\substack{1 \leq t \leq r \\ t \neq s}} \lambda_{t1} + L_s = \{x_{1\cdots 1 i_s 1 \cdots 1} \colon i_s = 1, \ldots, \ell_s\}$$

must be distinct and so (2.33) holds.

Let us fix s, with $s \leq r-1$, and also fix $i_{s+1}, \ldots, i_r$, with $(i_{s+1}, \ldots, i_r) \neq (1, \ldots, 1)$. Varying just the s^{th} place of the multi-index we have that the following $\ell_s - 1$ equalities on differences hold:

$$x_{1\cdots 1 i_s i_{s+1} \cdots i_r} - x_{1\cdots 1 1 i_{s+1} \cdots i_r} = \lambda_{s i_s} - \lambda_{s1} = x_{1 \cdots 1 i_s 1 \cdots 1} - x_{1\cdots 1}, \quad (i_s \neq 1),$$

We now vary $i_{s+1},\ldots,i_r$, and we have that the following $(\ell_{s+1}\cdots\ell_r-1)(\ell_s-1)$ equalities on sums hold:

$$x_{1\cdots1}+x_{1\cdots1i_si_{s+1}\cdots i_r}=x_{1\cdots1i_s1\cdots1}+x_{1\cdots1i_{s+1}\cdots i_r},\qquad \big(i_s\neq1,(i_{s+1},\ldots,i_r)\neq(1,\ldots,1)\big).$$

As this is true for $1\le s<r$ we have (2.34). Summing in s, the total number of equalities is

$$\begin{aligned}\sum_{s=1}^{r-1}(\ell_{s+1}\cdots\ell_r-1)(\ell_s-1)&=\sum_{s=1}^{r-1}(\ell_s\cdots\ell_r-\ell_{s+1}\cdots\ell_r-\ell_s+1)\\&=\ell_1\cdots\ell_r+\sum_{s=2}^{r-1}(-\ell_s\cdots\ell_r+\ell_s\cdots\ell_r)-\ell_r+\sum_{s=1}^{r-1}(-\ell_s+1)\\&=\ell_1\cdots\ell_r-(\ell_1+\cdots+\ell_r)+(r-1),\end{aligned}$$

as claimed.

To prove the second part of the lemma, suppose $X=\{x_{i_1\cdots i_r},\ 1\le i_s\le\ell_s, 1\le s\le r\}$ satisfies conditions (2.33) and (2.34). We define $L_1:=\{x_{11\cdots1},x_{21\cdots1},\ldots,x_{\ell_11\cdots1}\}$ and for $s=2,\ldots,r$ we define

$$L_s:=-x_{11\cdots1}+\{x_{1\cdots1i_s1\cdots1}\colon i_s=1,\ldots,\ell_s\}.$$

As $x_{1\cdots1}\in L_1$ and $0\in\cap_{s=2}^rL_s$ it is trivial that $x_{1\cdots1}=x_{1\cdots1}+\sum_{i=2}^r0$ belongs to both X and $L_1+\cdots+L_r$. In other case $(i_1,\ldots,i_r)\neq(1,\ldots,1)$ and then using $r-1$ times (2.34) we can write

$$\begin{aligned}x_{i_1\cdots i_r}&=x_{i_11\cdots1}-x_{1\cdots1}+x_{1i_2\cdots i_r}\\&=x_{i_11\cdots1}-x_{1\cdots1}+x_{1i_21\cdots1}-x_{1\cdots1}+x_{11i_3\cdots i_r}\\&\ \vdots\\&=x_{i_11\cdots1}+(-x_{1\cdots1}+x_{1i_21\cdots1})+\cdots+(-x_{1\cdots1}+x_{1\cdots1i_r}),\end{aligned}$$

which implies that any element of X (other than $x_{1\cdots1}$) belongs to $L_1+\cdots+L_r$ and vice versa. Hence we have $X=L_1+\cdots+L_r$. Condition (2.33) implies that $|L_s|=\ell_s$ $(1\le s\le r)$, and so $X\in\mathcal{L}^{(r)}_{\ell_1,\ldots\ell_r}$. □

Now we are ready to prove Proposition 2.1.

We take the projection $\varphi\colon \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \to \mathbb{Z}$ defined by

$$\varphi(x_1, \ldots, x_k) = x_1 + x_2(2n_1) + \cdots + x_k(2n_1)(2n_2)\cdots(2n_{k-1}).$$

We claim that φ preserves the property of being $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free.

Indeed, let $A \subset \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ be any set such that $\varphi(A)$ contains a sumset Y of the class $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$. We claim that $Z = \varphi^{-1}(Y)$ is a sumset of the class $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$ in the group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

By Lemma 2.11, Y can be multi-indexed $\{y_{i_1\cdots i_r}, : 1 \le i_s \le \ell_s, 1 \le s \le r\}$ and satisfies conditions (2.33) and (2.34).

By Lemma 2.4 the function φ is injective and so $\varphi^{-1}(Y) = Z$ can multi-indexed in the natural way : $z_{i_1\cdots i_r} = \varphi^{-1}(y_{i_1\cdots i_r})$. The map φ is injective and Y satisfies (2.33), hence we have that Z satisfies the conditions (2.33).

We have that Y satisfies (2.34) and by Lemma 2.4, the property (2.18) of φ holds. Therefore Z satisfies the equalities (2.34).

Hence the second part of Lemma 2.11 implies that $Z = \varphi^{-1}(Y)$ is a sumset of the class $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$ in the group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, as claimed.

Note that the image of φ is in the interval $[2^{k-1}n_1n_2\cdots n_k]$, because we have $x_i \le n_i - 1, (1 \le i \le k)$ and then

$$\begin{aligned}\varphi(x_1, \ldots, x_k) &\le (n_1 - 1) + (n_2 - 1)(2n_1) + (n_3 - 1)(2n_1)(2n_2) + \cdots \\ &= -1 + n_1 - 2n_1 + 2n_1n_2 - 4n_1n_2 + 4n_1n_2n_3 + \cdots \\ &= -1 - n_1 - 2n_1n_2 - \cdots - 2^{k-2}n_1n_2\cdots n_{k-1} + 2^{k-1}n_1n_2\cdots n_k \\ &< 2^{k-1}n_1n_2\cdots n_k.\end{aligned}$$

Therefore for any $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free set $A \subset \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ we have

$$|A| = |\varphi(A)| \le F(2^{k-1}n_1n_2\cdots n_k, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}),$$

which implies $F(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}) \le F(2^{k-1}n_1n_2\cdots n_k, \mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r})$.

2.4. Proofs of connections with problems on hyper-graphs and on matrices

2.4.1. Proof of Proposition 2.2

Proposition 2.2 *Let G be a finite abelian group with $|G| = n$. Then*

$$ex(n, K^{(r)}_{\ell_1,\dots,\ell_r}) \geq \binom{n}{r}\frac{F(G, \mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r})}{n}.$$

Let $A \subset G$ be any set free of subsets of the form $L_1 + \cdots + L_r$, with $|L_i| = \ell_i,\ i = 1, \dots, r$. Consider the hyper-graph $\mathcal{G} = (V, \mathcal{E})$ where $V = G$ and

$$\mathcal{E} = \left\{ \{x_1, \dots, x_r\} \in \binom{G}{r} :\ x_1 + \cdots + x_r \in A \right\}.$$

We claim that $\mathcal{G}$ does not contain a copy of the r-uniform hyper-graph $K^{(r)}_{\ell_1,\dots,\ell_r}$ (see definition 2.4). Otherwise there exist $L_1, \dots, L_r$ with $|L_i| = \ell_i,\ i = 1, \dots, r$, such that all the hyper-edges $\{x_1, \dots, x_r\}$ with $x_i \in L_i$ belong to $\mathcal{E}$. But this is equivalent to say that $x_1 + \cdots + x_r \in A$ for all $(x_1, \dots, x_r) \in L_1 \times \cdots \times L_r$. In other words, that $L_1 + \cdots + L_r \subset A$, which is not possible because A is $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free. Hence we have

$$\mathrm{ex}\left(n; K^{(r)}_{\ell_1,\dots,\ell_r}\right) \geq \#\left\{ \{x_1, \dots, x_r\} \in \binom{G}{r} :\ x_1 + \cdots + x_r \in A \right\},$$

an inequality which can be alternatively written as follows

$$\mathrm{ex}(n; K^{(r)}_{\ell_1,\dots,\ell_r}) \geq \sum_{y \in A} R_r(y),$$

where $R_r(y) = \#\{\{x_1, \dots, x_r\} \in \binom{G}{r} :\ x_1 + \cdots + x_r = y\}$.

Note that, for any given $x \in G$, as A is $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free then $A + x$ has the same property. This implies the last inequality also holds if we sum in

$y \in A + x$. Hence we can write

$$\begin{aligned}\mathrm{ex}(n; K^{(r)}_{\ell_1,\dots,\ell_r}) &\geq \frac{1}{|G|}\sum_{x\in G}\sum_{y\in A+x} R_r(y) = \frac{1}{|G|}\sum_{y\in G} R_r(y)\#\{x:\ x\in y-A\}\\ &= \frac{|A|}{|G|}\sum_{y\in G} R_r(y) = \frac{|A|}{|G|}\binom{|G|}{r} = \frac{|A|}{n}\binom{n}{r}.\end{aligned}$$

2.4.2. Proof of Theorem 2.6

Theorem 2.6 *For any $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$ we have*

$$ex(n, K^{(r)}_{\ell_1,\dots,\ell_r}) \leq \frac{(\ell_r - 1)^{1/\ell_1\cdots\ell_{r-1}}}{r!}\, n^{r-1/\ell_1\cdots\ell_{r-1}}(1+o(1)), \quad (n\to\infty).$$

The proof uses induction in r. The case $r = 2$ was proved by Kövari, Sós and Turán [31].

For $r \geq 3$ to ease the notation we write $e_r = ex(n, K^{(r)}_{\ell_1,\dots,\ell_r})$ and $e_{r-1} = ex(n, K^{(r-1)}_{\ell_2,\dots,\ell_r})$. Suppose $\mathcal{H} = (V, \mathcal{E})$ is one extreme r-hypergraph which is free of $K^{(r)}_{\ell_1,\dots,\ell_r}$ hypergraphs. We have

$$|\mathcal{E}| = e_r. \tag{2.35}$$

The neighbourhood of any vertex v in V is the collection of all $(r-1)$-subsets of V that form a r-hyperedge when combined with v:

$$N(v) = \left\{U \in \binom{V}{r-1} : \{v\}\cup U \in \mathcal{E}\right\}.$$

For any fixed ℓ_1 vertices $v_1, \dots, v_{\ell_1}$ let $\mathcal{E}'$ denote $N(v_1)\cap\cdots\cap N(v_{\ell_1})$. The set $\mathcal{E}'$ can be considered as a collection of $(r-1)$-hyperedges. Let $V' \subset V$ denote the vertices connected by $\mathcal{E}'$ thus forming a $(r-1)$-hypergraph $\mathcal{H}' = (V', \mathcal{E}')$. Assume that $\mathcal{H}'$ contains one $K^{(r-1)}_{\ell_2,\dots,\ell_r}$ hypergraph, say $\mathcal{I} = (V(\mathcal{I}), \mathcal{E}(\mathcal{I}))$. Then the hypergraph

$$(\{v_1, \dots, v_{\ell_1}\} \cup V(\mathcal{I}), \{\{v_i\} \cup U \mid U \in \mathcal{E}(\mathcal{I}),\ i = 1, \dots, \ell_1\})$$

would be r-uniform $K^{(r)}_{\ell_1,\dots,\ell_r}$ and it would be included in $\mathcal{H}$, which is impossible. Hence $(V',\mathcal{E}')$ must be $K^{(r-1)}_{\ell_2,\dots,\ell_r}$-free and so we have

$$|\mathcal{E}'| = |N(v_1)\cap\cdots\cap N(v_{\ell_1})| \le e_{r-1} \quad \text{for any } v_1,\dots,v_{\ell_1}. \tag{2.36}$$

In order to use Theorem 2.10, let us define the random variable $X\colon V \to \binom{V}{r-1}$ with uniform probability law $\mathbb{P}(X=U) = 1/\binom{n}{r-1}$, for every $U \in \binom{V}{r-1}$. For any $v\in V$ we define the event $E_v = \{X \in N(v)\}$. Note that $\sum_{v\in V}|N(v)|$ counts the number of all subsets of $r-1$ elements in every hyperedge of V, thus $\sum_{v\in V}|N(v)| = \binom{r}{r-1}|\mathcal{E}|$ and then we can write

$$\sigma_1 = \sum_{v\in V}\mathbb{P}(E_v) = \frac{1}{\binom{n}{r-1}}\sum_{v\in V}|N(v)| = \frac{r\,|\mathcal{E}|}{\binom{n}{r-1}} = \frac{r\,e_r}{\binom{n}{r-1}},$$

where in the last equality we have used (2.35). Theorem 2.10 implies

$$\frac{1}{\binom{n}{r-1}}\sum_{\{v_1,\dots,v_{\ell_1}\}\in\binom{V}{\ell_1}} |N(v_1)\cap\cdots\cap N(v_{\ell_1})| \ge \binom{r\,e_r/\binom{n}{r-1}}{\ell_1}.$$

Using the inequality (2.36) we obtain

$$\frac{\binom{n}{\ell_1}\,e_{r-1}}{\binom{n}{r-1}} \ge \binom{r\,e_r/\binom{n}{r-1}}{\ell_1}. \tag{2.37}$$

Now we estimate the left term in (2.37):

$$\frac{e_{r-1}\binom{n}{\ell_1}}{\binom{n}{r-1}} = \frac{(r-1)!}{\ell_1!}\frac{(n-(r-1))!}{(n-\ell_1)!}\,e_{r-1}.$$

In the case $r-1\le \ell_1$ we have

$$\frac{e_{r-1}\binom{n}{\ell_1}}{\binom{n}{r-1}} = \frac{(r-1)!}{\ell_1!}\,e_{r-1}(n-r+1)\cdots(n-\ell_1+1) \le \frac{(r-1)!}{\ell_1!}\,e_{r-1}\,n^{\ell_1-r+1}.$$

Otherwise we have $r-1>\ell_1$ and then

$$\begin{aligned}\frac{e_{r-1}\binom{n}{\ell_1}}{\binom{n}{r-1}} &= \frac{(r-1)!}{\ell_1!}\,\frac{e_{r-1}}{(n-\ell_1)\cdots(n-r+2)} \le \frac{(r-1)!}{\ell_1!}\,\frac{e_{r-1}}{(n-r+2)^{r-1-\ell_1}}\\ &\le \frac{(r-1)!}{\ell_1!}\,e_{r-1}\,(n-r+2)^{\ell_1-r+1}.\end{aligned}$$

Hence we have

$$\frac{e_{r-1}\binom{n}{\ell_1}}{\binom{n}{r-1}} \le \frac{(r-1)!}{\ell_1!}\, e_{r-1}\, n^{\ell_1-r+1}(1+o(1)), \quad (n\to\infty).$$

A lower bound for the right term in (2.37) is

$$\binom{r\, e_r/\binom{n}{r-1}}{\ell_1} \ge \binom{\frac{r!\,e_r}{n^{r-1}}}{\ell_1} \ge \frac{\left(\frac{r!\,e_r}{n^{r-1}} - (\ell_1-1)\right)^{\ell_1}}{\ell_1!}.$$

Combining the last two estimates and (2.37) we can write

$$\left(\frac{r!\,e_r}{n^{r-1}} - (\ell_1-1)\right)^{\ell_1} \le (r-1)!\,e_{r-1}\,n^{\ell_1-r+1}(1+o(1)), \qquad (n\to\infty). \tag{2.38}$$

By (2.10) we have that $e_r \gg n^{r-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}}$. The fraction in this last exponent reaches its maximum for $r=\ell_1=\ell_2=2$, that is to say $\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1} \le \frac{2}{3}$. Hence $e_r/n^{r-1} \gg n^{1/3} \to \infty$, and then we have that $\ell_1 - 1 = o\left(e_r/n^{r-1}\right)$, $(n\to\infty)$, which implies

$$\left(\frac{r!\,e_r}{n^{r-1}} - (\ell_1-1)\right)^{\ell_1} = \left(\frac{r!\,e_r}{n^{r-1}}\right)^{\ell_1}(1+o(1)), \quad (n\to\infty).$$

Using this last equality and (2.38) we can write

$$\left(\frac{r!\,e_r}{n^{r-1}}\right)^{\ell_1}(1+o(1)) \le (r-1)!\,e_{r-1}\,n^{\ell_1-r+1}(1+o(1)), \qquad (n\to\infty),$$

and so

$$\begin{aligned} e_r &\le \frac{n^{r-1}}{r!}\big((r-1)!\big)^{1/\ell_1}(e_{r-1})^{1/\ell_1}\,n^{1-\frac{r-1}{\ell_1}}(1+o(1)) \\ &\le \frac{\big((r-1)!\big)^{1/\ell_1}}{r!}(e_{r-1})^{1/\ell_1}\,n^{r-\frac{r-1}{\ell_1}}(1+o(1)), \quad (n\to\infty). \end{aligned} \tag{2.39}$$

To prove the induction step assume that (2.12) holds for $r-1$, then

$$e_{r-1} \le \frac{(\ell_r-1)^{1/\ell_2\cdots\ell_{r-1}}}{(r-1)!}\,n^{r-1-1/\ell_2\cdots\ell_{r-1}}(1+o(1)), \qquad (n\to\infty),$$

and inserting this into (2.39) we have

$$\begin{aligned} e_r &\le \frac{((r-1)!)^{1/\ell_1}}{r!}\left(\frac{(\ell_r-1)^{1/\ell_2\cdots\ell_{r-1}}}{(r-1)!}\,n^{r-1-1/\ell_2\cdots\ell_{r-1}}(1+o(1))\right)^{1/\ell_1} n^{r-\frac{r-1}{\ell_1}} \\ &\le \frac{(\ell_r-1)^{1/\ell_1\cdots\ell_{r-1}}}{r!}\,n^{r-1/\ell_1\cdots\ell_{r-1}}(1+o(1)), \qquad (n\to\infty). \end{aligned}$$

Hence (2.12) also holds for r and the proof of Theorem 2.6 is completed.

2.4.3. Proofs of Proposition 2.3 and of Corollary 2.1

Proof of Proposition 2.3

Recall definitions 2.5 and 2.6 on page 59.

Proposition 2.3 *Given a hypergraph $\mathcal{H}$, let $ex(n, \mathcal{H})$ denote the maximum number of hyperedges of a n vertices hypergraph which does not contain $\mathcal{H}$ as a sub-hypergraph. Let P be any given 0-1 matrix. Then we have*

$$f(n, P, d) = ex(dn, \mathcal{G}(P)).$$

Assume that a d-dimensional $n \times \cdots \times n$ zero-one matrix A avoids P. Then $\mathcal{G}(A)$ has dn vertices and it is free of $\mathcal{G}(P)$. The number of ones in A is the same as the number of hyper-edges in $\mathcal{G}(A)$ which is bounded by $\mathrm{ex}(dn, \mathcal{G}(P))$. Then we can write

$$f(n, P, d) = \max_{A \text{ avoids } P} (\text{number of ones in } A) \leq \mathrm{ex}(dn, \mathcal{G}(P)).$$

Let $G = (V, \mathcal{E})$ be any hyper-graph with dn vertices and free of $\mathcal{G}(P)$. Then $\mathcal{M}(G)$ is a $n \times \cdots \times n$ zero-one matrix that avoids P, and it has $|\mathcal{E}|$ ones, hence $|\mathcal{E}| \leq f(n, P, d)$. Thus

$$\mathrm{ex}(dn, \mathcal{G}(P)) = \max_{\substack{(V,\mathcal{E}) \text{ free of } \mathcal{G}(P) \\ |V| = dn}} (|\mathcal{E}|) \leq f(n, P, d).$$

Proof of Corollary 2.1

Corollary 2.1 *Let $2 \leq k_1 \leq k_2 \leq \cdots \leq k_d$. Then we have*

$$f(n, R^{k_1,\ldots,k_d}, d) \leq \frac{(k_d - 1)^{\alpha} d^{d-\alpha}}{d!} n^{d-\alpha}(1 + o(1)), \quad \textit{where } \alpha = \frac{1}{k_1 k_2 \cdots k_{d-1}}.$$

The matrix $R^{k_1,\dots,k_d}$ corresponds to the d-partite d-uniform complete hypergraph $K^{(d)}_{k_1,\dots,k_d}$, that is to say $\mathcal{G}(R^{k_1,\dots,k_d}) = K^{(d)}_{k_1,\dots,k_d}$ (see definition 2.6). Proposition 2.3 implies

$$f(n, R^{k_1,\dots,k_d}, d) = \mathrm{ex}(dn, K^{(d)}_{k_1,\dots,k_d}). \tag{2.40}$$

Theorem 2.6 provides an upper bound for the right term in this equality, and so we can write

$$\begin{aligned} f(n, R^{k_1,\dots,k_d}, d) &\le \frac{(k_d-1)^{1/k_1k_2\cdots k_{d-1}}}{d!}\,(dn)^{d-1/k_1k_2\cdots k_{d-1}}(1+o(1)) \\ &= \frac{(k_d-1)^{\alpha}d^{d-\alpha}}{d!}\,n^{d-\alpha}(1+o(1)). \end{aligned}$$

2.5. Proofs of results for infinite $\mathcal{L}$-free sequences of integers

2.5.1. Proof of Theorem 2.7

Theorem 2.7 *If A is an infinite $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free sequence then*

$$\liminf_{x\to\infty} \frac{A(x)}{x}(x\log x)^{1/(\ell_1\cdots\ell_{r-1})} \ll 1.$$

We part the interval $(0, N^2]$ into the subintervals $I_j = ((j-1)N, jN]$, $j = 1,\dots,N$ and use the notation $A_j = A\cap I_j$. Note that $A(tN) = \sum_{j\le t}|A_j|$, $(1 \le t \le N)$. We will first estimate the sum

$$S = \sum_{j=1}^{N} \frac{|A_j|}{j^{1-1/(\ell_1\cdots\ell_{r-1})}}.$$

Let $\sigma(x)$ denote the number $\inf_{y>x} A(y)\dfrac{(y\log y)^{1/(\ell_1\cdots\ell_{r-1})}}{y}$.

On the one hand for any t such that $1\le t\le N$ we have

$$A(tN) \ge \frac{\sigma(N)(tN)^{1-1/(\ell_1\dots\ell_{r-1})}}{(\log(tN))^{1/(\ell_1\dots\ell_{r-1})}} \ge \frac{\sigma(N)(tN)^{1-1/(\ell_1\dots\ell_{r-1})}}{(2\log N)^{1/(\ell_1\dots\ell_{r-1})}}.$$

We use this inequality and summation by parts to get

$$
\begin{aligned}
S &\geq (1-1/(\ell_1\cdots\ell_{r-1}))\int_1^N \frac{\sum_{j\leq t}|A_j|}{t^{2-1/(\ell_1\cdots\ell_{r-1})}}\,\mathrm{d}t\\
&\geq \frac{1}{2}\int_1^N \frac{A(tN)}{t^{2-1/(\ell_1\cdots\ell_{r-1})}}\,\mathrm{d}t\\
&\geq \frac{\sigma(N)N^{1-1/(\ell_1\cdots\ell_{r-1})}}{4(\log N)^{1/(\ell_1\dots\ell_{r-1})}}\int_1^N \frac{\mathrm{d}t}{t}\\
&\geq \frac{\sigma(N)}{4}\left(N\log N\right)^{1-1/(\ell_1\cdots\ell_{r-1})}. \qquad (2.41)
\end{aligned}
$$

On the other hand Hölder inequality yields

$$
S \leq \left(\sum_{j=1}^N |A_j|^{\ell_1\cdots\ell_{r-1}}\right)^{1/(\ell_1\cdots\ell_{r-1})}\left(\sum_{j=1}^N \frac{1}{j}\right)^{1-1/(\ell_1\cdots\ell_{r-1})}.
$$

At this point we will need the following result.

Lemma 2.12. *Let $A\subset\mathbb{Z}$ be $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free and $A_j = A\cap((j-1)N, jN],\ j = 1,\dots,N$. Then we have*

$$
\sum_{j\leq N}|A_j|^{\ell_1\cdots\ell_{r-1}} \ll N^{\ell_1\cdots\ell_{r-1}-1}.
$$

Assuming Lemma 2.12 holds (we will prove it below) we can write

$$
S \ll N^{1-1/(\ell_1\cdots\ell_{r-1})}(\log N)^{1-1/(\ell_1\cdots\ell_{r-1})}. \qquad (2.42)
$$

Inequalities (2.41) and (2.42) imply $\sigma(N)\ll 1$ that is precisely the claim of Theorem 2.7.

Proof of Lemma 2.12. We use induction on r. We will call ℓ_1-subsets to the subsets of ℓ_1 elements.

When $r=2$ then $\sum_{j\leq N}\binom{|A_j|}{\ell_1}$ counts the ℓ_1-subsets in A included in one of the intervals $I_j = ((j-1)N, jN],\ j = 1,\dots,N$. We will estimate this number in two steps. On the one hand there are $\binom{N-1}{\ell_1-1}$ classes of pairwise congruent ℓ_1-subsets of A with diameter less than N. The reason is that each of these classes contains a representative subset that is within $[1,N]$

and which contains 1, note that the remaining elements of the representative subset can be chosen in $\binom{N-1}{\ell_1-1}$ different ways. On the other hand it is easy to see that since A is $\mathcal{L}_{\ell_1,\ell_2}$-free then necessarily every class of pairwise congruent ℓ_1-subsets contains at most ℓ_2 members. Hence we have

$$\sum_{j\le N}|A_j|^{\ell_1}\ll\sum_{j\le N}\binom{|A_j|}{\ell_1}\le\ell_2\binom{N-1}{\ell_1-1}\ll N^{\ell_1-1}.$$

When $r\ge 3$ assume that Lemma 2.12 is true for $r-1$. For any set S and any collection $x=\{x_1,\dots,x_{\ell_1}\}\in\binom{N}{\ell_1}$ we will use the notation $S*x=\bigcap_{i=1}^{\ell_1}(S+x_i)$.

On the one hand Hölder inequality yields

$$\sum_{x\in\binom{N}{l_1}}|A_j*x|\le\left(\sum_{x\in\binom{N}{l_1}}|A_j*x|^{\ell_2\cdots\ell_{r-1}}\right)^{1/(\ell_2\cdots\ell_{r-1})}\binom{N}{\ell_1}^{1-1/(\ell_2\cdots\ell_{r-1})}. \tag{2.43}$$

On the other hand Lemma 2.6 with $X=[2N]$ and $B=[N]$ implies

$$\sum_{x\in\binom{N}{\ell_1}}|A_j*x|\ge 2N\binom{|A_j|/2}{\ell_1}\gg N|A_j|^{\ell_1}. \tag{2.44}$$

Combining (2.43) and (2.44) we obtain

$$N^{\ell_2\cdots\ell_{r-1}}|A_j|^{\ell_1\cdots\ell_{r-1}}\ll\left(\sum_{x\in\binom{N}{\ell_1}}|A_j*x|^{\ell_2\cdots\ell_{r-1}}\right)N^{\ell_1\cdots\ell_{r-1}-\ell_1}$$

Summing in j we can write:

$$N^{\ell_2\cdots\ell_{r-1}}\sum_{j\le N}|A_j|^{\ell_1\cdots\ell_{r-1}}\ll N^{\ell_1\cdots\ell_{r-1}-\ell_1}\sum_{x\in\binom{N}{\ell_1}}\sum_{j\le N}|A_j*x|^{\ell_2\cdots\ell_{r-1}}$$

Observe that A_j is $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$-free (because $A_j\subset A$) and then Lemma 2.1 implies that for any $x=\{x_1,\dots,x_{\ell_1}\}\in\binom{N}{\ell_1}$ the set $A_j*x=\bigcap_{i=1}^{\ell_1}(A_j+x_i)$ is $\mathcal{L}^{(r-1)}_{\ell_2,\dots,\ell_r}$-free. Hence we apply the induction hypothesis to each A_j*x to obtain

$$N^{\ell_2\cdots\ell_{r-1}}\sum_{j\le N}|A_j|^{\ell_1\cdots\ell_{r-1}}\ll N^{\ell_1\cdots\ell_{r-1}-\ell_1}\sum_{x\in\binom{N}{\ell_1}}N^{\ell_2\cdots\ell_{r-1}-1}$$

Thus we have

$$\sum_{j\le N} |A_j|^{\ell_1\cdots\ell_{r-1}} \ll N^{\ell_1\cdots\ell_{r-1}-1},$$

as claimed. □

2.5.2. Proofs of Theorems 2.8 and 2.9

Theorem 2.8 *For any $\ell \ge 2$ and for any $\epsilon > 0$ there exists an infinite $\mathcal{L}_{2,\ell}$-free sequence with*

$$A(x) \gg x^{1-\frac{\ell}{2\ell-1}-\epsilon}.$$

Theorem 2.9 *For any $r \ge 2$ and for any $\epsilon > 0$ there exists an infinite $\mathcal{L}^{(r)}_{2,\dots,2}$-free sequence with*

$$A(x) \gg x^{1-\frac{r}{2^r-1}-\epsilon}.$$

The strategy of the proof is the same for the two cases of Hilbert cubes and $\mathcal{L}_{2,\ell}$. We first construct a dense random sequence S free of arithmetic progressions. We will say that X is an *obstruction* (for S) when $X \subset S$ is a sumset of the class $\mathcal{L}^{(r)}_{\ell_1,\dots,\ell_r}$. The sequence S is likely to have infinitely many obstructions. If we could prove that obstructions are few then we would be able to remove all of them by just removing few elements from S. After the removal process we would retain a subsequence $A \subset S$ satisfying the conditions of Theorem 2.8 (resp. Theorem 2.9). Thus we have to estimate the number of obstructions for S. In the cases of Hilbert cubes and $\mathcal{L}_{2,\ell}$ we have succeeded to obtain an upper bound which allows to complete the proofs of Theorems 2.9 and 2.8.

Our first remark is that we can take ϵ as little as needed in the sense that if Theorem 2.8 is true for a particular $\epsilon_0 > 0$ then it is also true for any $\epsilon > \epsilon_0$.

We define a collection of intervals as follows:

$$I_m = [4^{m+2}, 4^{m+2} + 4^m), \quad (m \geq 1).$$

Let B_m denote the set given by Theorem 2.11 of Behrend with the following properties: $B_m \subset I_m$, B_m is free of arithmetic progressions and has size $|B_m| \geq 4^{m(1+o(1))}$.

Given $\epsilon > 0$ we have $|B_m| \geq 4^{m(1-\epsilon/2)}$, $(m \geq m_\epsilon)$, for some positive integer m_ϵ. We take

$$B = \bigcup_{m \geq m_\epsilon} B_m.$$

Let $r, \ell_1, \dots, \ell_r$ be integers with $r \geq 2$ and $2 \leq \ell_1 \leq \cdots \leq \ell_r$. We consider the probability space of all random infinite sequences S of positive integers with law

$$\mathbb{P}(\nu \in S) = \begin{cases} f(\nu) \text{ if } \nu \in B, \\ 0 \text{ otherwise,} \end{cases}$$

where all the events $\{\nu \in S\}_{\nu \geq 1}$ are mutually independent and

$$f(\nu) = \nu^{-\alpha}, \qquad \alpha = \frac{\ell_1 + \cdots + \ell_r - r}{\ell_1 \cdots \ell_r - 1} + \epsilon/2.$$

We will write S_m for the intersection $S \cap B_m$.

Lemma 2.13. *Any random sequence S defined as above is free of arithmetic progressions and with high probability we have*

$$|S_m| \gg 4^{m\left(1 - \frac{\ell_1 + \cdots + \ell_r - r}{\ell_1 \cdots \ell_r - 1} - \epsilon\right)}, \quad (m \to \infty). \tag{2.45}$$

Proof. As $S \subset B$, it suffices to proof that the set B does not contain arithmetic progressions. Take any $x_1 < x_2 < x_3$ with $x_1 \in B_{m_1},\ x_2 \in B_{m_2},\ x_3 \in B_{m_3}$ and $m_1 \leq m_2 \leq m_3$. If $m_1 = m_2 = m_3$ then x_1, x_2, x_3 are not in arithmetic progression because B_{m_1} is free of them.

If $m_1 < m_2 < m_3$ and $2x_2 = x_1 + x_3$ then we would have

$$34 \cdot 4^{m_2} = 2(4^{m_2+2} + 4^{m_2}) \geq 2x_2 = x_1 + x_3 \geq 4^{m_3+2} \geq 4^{m_2+3} = 64 \cdot 4^{m_2},$$

which is false. If $m_1 < m_2 = m_3$ then

$$x_2 - x_1 \geq 4^{m_2+2} - (4^{m_2+1} + 4^{m_2-1}) = \frac{47}{4} 4^{m_2} > x_3 - x_2,$$

and then x_1, x_2, x_3 are not in arithmetic progression. If $m_1 = m_2 < m_3$ then

$$x_3 - x_2 \geq 4^{m_2+3} - (4^{m_2+2} + 4^{m_2}) = 47 \cdot 4^{m_2} > x_2 - x_1,$$

and then x_1, x_2, x_3 are not in arithmetic progression.

When $\nu \in B_m$ then $\nu < 4^{m+3}$ and so the expected size of $S_m = S \cap B_m$ is

$$\mu_m = \mathbb{E}(|S_m|) = \sum_{\nu \in B_m} \nu^{-\alpha} \geq |B_m| 4^{-(m+3)\alpha} \gg 4^{m(1-\epsilon/2-\alpha)}, \quad (m \to \infty).$$

Since $|S_m|$ is a sum of mutually independent indicator random variables we can apply Chernoff inequality to obtain

$$\mathbb{P}(|S_m| < \mu_m/2) < e^{-\mu_m/2} \ll e^{-4^{m(1-\epsilon/2-\alpha)}}.$$

This inequality implies $\sum_{m \geq 3} \mathbb{P}(|S_m| < \mu_m/2) < \infty$, and then by the Borell-Cantelli Lemma we have that with high probability

$$|S_m| \geq \mu_m/2 \gg 4^{m(1-\epsilon/2-\alpha)} = 4^{m(1-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}-\epsilon)}, \quad (m \to \infty).$$

$\square$

We want to prune the sequence S in order to destroy all obstructions. To this end we will remove from every obstruction its greatest element. Let S_m^{bad} denote the collection of all elements in S_m that have the property to be the greatest element in at least one obstruction (to S):

$$S_m^{\text{bad}} := \{s \in S_m \mid s = \max(X),\ X \subset S \text{ is an obstruction}\}.$$

We also define a random variable that counts the number of obstructions that have their maximum in S_m:

$$N(S_m) := \{X \subset S \text{ is an obstruction } \mid \max(X) \in S_m\}.$$

For two particular cases we claim that obstructions with a maximum in S_m are few.

Lemma 2.14. *For the two cases $\mathcal{L}_{2,\ell}$ and $\mathcal{L}^{(r)}_{2,\ldots,2}$ we have with high probability*

$$|N(S_m)| = o(|S_m|), \quad (m \to \infty). \tag{2.46}$$

We postpone the proof of Lemma 2.14 until the end of this section.

Now we can end the proof of Theorems 2.8 and 2.9 as follows. Take the randomly constructed sequence S. For every obstruction $X \subset S$ we have that $\max(X) \in S_m$ for some m. We remove $\max(X)$ from the set S_m. We perform this removal process for all the obstructions for S. Let S_m^* denote the subset of S_m that is retained after the completion of this removal process. Two different obstructions might have the same maximum therefore $N(S_m) \geq |S_m^{\mathrm{bad}}|$. Thus by Lemma 2.13 and Lemma 2.14, with high probability we have that the retained elements are at least

$$|S_m^*| = |S_m \setminus S_m^{\mathrm{bad}}| \geq |S_m| - |N(S_m)| \gg |S_m| \gg 4^{m(1-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}-\epsilon)}, \quad (m \to \infty),$$

for the two cases $\mathcal{L}_{2,\ell}$ and $\mathcal{L}^{(r)}_{2,\ldots,2}$.

Finally let us take $A = \bigcup_{m\geq m_\epsilon} S_m^*$. On the one hand A is $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$-free because all sumsets of the class $\mathcal{L}^{(r)}_{\ell_1,\ldots,\ell_r}$ that were contained in the initial sequence S have been destroyed in the process of obtaining the subsequence $A \subset S$.

On the other hand for each x large enough take the integer k such that $4^k < x \leq 4^{k+1}$. It is clear that

$$A(x) \geq \sum_{m\leq k} |S_m^*| \geq |S_k^*| \gg 4^{k(1-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}-\epsilon)} \gg x^{1-\frac{\ell_1+\cdots+\ell_r-r}{\ell_1\cdots\ell_r-1}-\epsilon}, \quad (x \to \infty),$$

holds, with high probability, for the two cases $\mathcal{L}_{2,\ell}$ and $\mathcal{L}^{(r)}_{2,\ldots,2}$. Therefore at least one sequence must exist satisfying Theorem 2.8. The same applies for Theorem 2.9.

In the proof of Lemma 2.14 we will use the following well known estimates:

$$\sum_{n\leq x} n^\beta \asymp x^{1+\beta} \quad \text{if } \beta > -1. \tag{2.47}$$

$$\sum_{x\leq n} n^\beta \asymp x^{1+\beta} \quad \text{if } \beta < -1. \tag{2.48}$$

Proof of Lemma 2.14 for the case $\mathcal{L}_{2,\ell}$

Any sumset X in $\mathcal{L}_{2,\ell}$ can be described as follows:

$$X = \{0, x\} + \{y_1, \ldots, y_\ell\}, \qquad y_1 \leq \cdots \leq y_\ell.$$

For any fixed choice of $x, y_1, \ldots, y_\ell$ either (a) there exists a t with $2 \leq t \leq \ell$ such that

$$y_1 \leq \cdots \leq y_{t-1} \leq x \leq y_t \leq \cdots \leq y_\ell, \tag{2.49}$$

or alternatively (b) we have either $x \leq y_1 \leq \cdots \leq y_\ell$ (type "left") or $y_1 \leq \cdots \leq y_\ell \leq x$ (type "right"). For convenience we will say that X is "of type t" when $X = \{0, x\} + \{y_1, \ldots, y_\ell\}$ and (2.49) holds.

Suppose that a sumset X of the class $\mathcal{L}_{2,\ell}$ is contained in S. By Lemma 2.13, S does not contain arithmetic progressions, hence X is also free of them. Then Lemma 2.2 implies that X cannot be degenerate, that is to say all the possible sums that contribute to the sumset X are distinct (see Definition 2.7). Hence

$$P(X \subset S) = f(y_1) \cdots f(y_\ell) f(x + y_1) \cdots f(x + y_\ell).$$

We will estimate first the expected number of obstructions X (to S) such that $\max(X) \in S_m$ for the cases left and right.

Let N_m^L denote the number of number of such obstructions that satisfy $x \leq y_1 \leq \cdots \leq y_\ell$. The function $f(\nu) = \nu^{-\alpha}$, where $\alpha = \frac{l}{2l-1} + \epsilon/2$, is non-increasing so $f(x + y_i) \leq f(y_i)$, and we can write

$$P(X \subset S) = f(y_1) \cdots f(y_\ell) f(x + y_1) \cdots f(x + y_\ell) \leq f(y_1)^2 \cdots f(y_\ell)^2.$$

Note also that if $x + y_\ell = \max(X) \in S_m \subset [4^{m+2}, 4^{m+2} + 4^m)$ then $y_\ell \leq 4^{m+3}$. Hence we can write

$$\begin{aligned}
\mathbb{E}\left(N_m^L\right) &= \sum_{\substack{X \text{ of type left end} \\ \max(X) \in S_m}} \mathbb{P}\left(X \subset S\right) \\
&\leq \sum_{x \leq y_1 \leq \cdots \leq y_\ell \leq 4^{m+3}} f(y_1)^2 \cdots f(y_\ell)^2 = \sum_{x \leq y_1 \leq \cdots \leq y_\ell \leq 4^{m+3}} y_1^{-2\alpha} \cdots y_\ell^{-2\alpha} \\
&\leq \sum_{x \leq 4^{m+3}} \left(\sum_{x \leq y} y^{-2\alpha} \right)^\ell \ll \sum_{x \leq 4^{m+3}} x^{(1-2\alpha)\ell} \ll 4^{m(1+(1-2\alpha)\ell)},
\end{aligned}$$

where, since $2\alpha = \frac{2l}{2l-1} + \epsilon > 1$ and $2\alpha - 1 = \frac{1}{2l-1} + \epsilon < 1$ for ϵ small enough, we have used the estimates (2.47) and (2.48).

Let N_m^R denote the number number of obstructions X (to S) such that $\max(X) \in S_m$, with $y_1 \le \cdots \le y_\ell \le x$. Again by the monotony of f we have

$$P(X \subset S) = f(y_1)\cdots f(y_\ell)f(x+y_1)\cdots f(x+y_\ell) \le f(y_1)\cdots f(y_\ell)f(x)^\ell,$$

and then

$$\begin{aligned}\mathbb{E}\left(N_m^R\right) &= \sum_{\substack{X \text{ of type right end} \\ \max(X)\in S_m}} \mathbb{P}\left(X \subset S\right) \\ &\le \sum_{y_1\le\cdots y_\ell\le x\le 4^{m+3}} f(y_1)\cdots f(y_\ell)f(x)^\ell = \sum_{y_1\le\cdots y_\ell\le x\le 4^{m+3}} y_1^{-\alpha}\cdots y_\ell^{-\alpha}x^{-\alpha\ell} \\ &\le \sum_{x\le 4^{m+3}}\left(\sum_{y\le x} y^{-\alpha}\right)^\ell x^{-\alpha\ell} \ll \sum_{x\le 4^{m+3}} x^{(1-2\alpha)\ell} \ll 4^{m(1+(1-2\alpha)\ell)},\end{aligned}$$

where we have taken ϵ sufficiently small to have $\alpha < 1$.

Fix t with $2 \le t \le \ell$. By (2.49) and the monotony of the function f we have:

$$f(x+y_i) \le f(x),\ (1 \le i \le t-1), \qquad f(x+y_i) \le f(y_i),\ (t \le i \le \ell).$$

Then we can write

$$\begin{aligned}\mathbb{P}\left(X \subset S\right) &\le f(y_1)\cdots f(y_\ell)f(x)^{t-1}f(y_t)\cdots f(y_\ell) \\ &= f(y_1)\cdots f(y_{t-1})f(x)^{t-1}f(y_t)^2\cdots f(y_\ell)^2.\end{aligned}$$

Let $N_m^{(t)} = N_m^{(t)}(S)$ denote the number of sumsets X of type t such that $X \subset S$ and $\max(X) \in S_m$. The expected value of $N_m^{(t)}$ can be estimated as follows

$$\begin{aligned}
\mathbb{E}\left(N_m^{(t)}\right) &= \sum_{\substack{X \text{ of type } t\\ \max(X)\in S_m}} \mathbb{P}\left(X\subset S\right)\\
&\le \sum_{\substack{y_1\le\cdots\le y_{t-1}\le x\\ x\le y_t\le\cdots\le y_\ell\le 4^{m+3}}} f(y_1)\cdots f(y_{t-1})f(x)^{t-1}f(y_t)^2\cdots f(y_\ell)^2\\
&\le \sum_{\substack{y_1,\ldots,y_{t-1}\le x\\ x\le y_t\le\cdots\le y_\ell\le 4^{m+3}}} y_1^{-\alpha}\cdots y_{t-1}^{-\alpha}x^{-(t-1)\alpha}y_t^{-2\alpha}\cdots\le y_\ell^{-2\alpha}\\
&\le \sum_{x\le y_t\le\cdots y_\ell\le 4^{m+3}} \left(\sum_{y\le x} y^{-\alpha}\right)^{t-1} x^{-(t-1)\alpha}y_t^{-2\alpha}\cdots y_\ell^{-2\alpha}\\
&\le \sum_{x\le 4^{m+3}} x^{-(t-1)\alpha}\left(\sum_{x\le y} y^{-2\alpha}\right)^{\ell-t+1}\left(\sum_{y\le x} y^{-\alpha}\right)^{t-1}\\
\left(\text{since } \tfrac{1}{2}<\alpha<1 \text{ for } \epsilon \text{ small}\right) &\le \sum_{x\le 4^{m+3}} x^{-(t-1)\alpha}x^{(1-2\alpha)(\ell-t+1)}x^{(1-\alpha)(t-1)}\\
&\le \sum_{x\le 4^{m+3}} x^{-(2\alpha-1)\ell} \ll 4^{m(1-(2\alpha-1)\ell)},
\end{aligned}$$

since $(2\alpha-1)\ell=\frac{\ell}{2\ell-1}+\epsilon\ell<1$ for ϵ small enough. Observe that $N(S_m)=N_m^L+\sum_{t=2}^{\ell}N_m^{(t)}+N_m^R$, hence we can write

$$\mathbb{E}\left(N(S_m)\right)=\mathbb{E}\left(N_m^L\right)+\sum_{t=2}^{\ell}\mathbb{E}\left(N_m^{(t)}\right)+\mathbb{E}\left(N_m^R\right)\ll 4^{m(1+(1-2\alpha)\ell)}.$$

Markov inequality yields

$$\sum_{m\ge m_\epsilon}\mathbb{P}\left(N(S_m)>m^2\mathbb{E}(N(S_m))\right)\le\sum_{m\ge m_\epsilon}\frac{1}{m^2}<\infty.$$

Thus by the Borell-Cantelli Lemma with high probability we have

$$N(S_m)\ll m^2\mathbb{E}\left(N(S_m)\right)\ll 4^{m(1+(1-2\alpha)\ell+o(1))}=4^{m(1-\frac{\ell}{2\ell-1}-\ell\epsilon+o(1))}.$$

Using this and the estimate (2.45) we have with high probability

$$\frac{N(S_m)}{|S_m|}\ll 4^{m((1-\ell)\epsilon+o(1))}\to 0,\quad (m\to\infty),$$

since $\ell\ge 2$, which proves Lemma 2.14 for the case $\mathcal{L}_{2,\ell}$.

Proof of Lemma 2.14 for the case of Hilbert cubes

Any Hilbert cube X of dimension r can be written as

$$X = x_0 + \{0, x_1\} + \cdots + \{0, x_r\}, \quad (x_1 \leq \cdots \leq x_r).$$

Indeed if $X = L_1 + \cdots + L_r$ with $L_j = \{a_j, b_j\}$, take $x_0 = \sum_{j=1}^{r} a_j$ and $x_j = b_j - a_j$, rearranging the indexes if needed to have $x_1 \leq \cdots \leq x_r$. In other words, $X = \{x_0 + \sum_{i \in I} x_i \mid I \subset [r]\}$, where the indexes in the sum cover all subsets of the interval $[r] = \{1, \ldots, r\}$.

Suppose that a Hilbert cube X is contained in S. By Lemma 2.13, S does not contain arithmetic progressions, hence X is also free of them. Then Lemma 2.2 implies that X cannot be degenerate, that is to say all the possible sums that contribute to the sumset X are distinct (see Definition 2.7).

For any fixed choice of $x_0, x_1, \ldots, x_r$ with $x_1 \leq \cdots \leq x_r$, the probability that the corresponding Hilbert cube $X = \{x_0 + \sum_{i \in I} x_i \mid I \subset [r]\}$ is contained in the random infinite sequence S is

$$\begin{aligned}\mathbb{P}\left(X \subset S\right) &= \mathbb{P}\left(\bigwedge_{I \subset [r]} (x_0 + \sum_{i \in I} x_i \in S)\right) = \prod_{I \subset [r]} \mathbb{P}\left(x_0 + \sum_{i \in I} x_i \in S\right) \\ &= \prod_{I \subset [r]} \left(x_0 + \sum_{i \in I} x_i\right)^{-\alpha},\end{aligned}$$

because all the sums $x_0 + \sum_{i \in I} x_i$ are distinct. The indexes I in the sum (and in the product) cover all subsets of the interval $[r]$, that is to say: $\emptyset$, and -for each $i = 1, \ldots, r$- all the 2^{i-1} subsets of $[r]$ in which i is the maximum. Note that having fixed i, for each s-uple $k_1, \cdots, k_s$ with $1 \leq k_1 \leq \cdots \leq k_s \leq i$ we have

$$(x_0 + x_{k_1} + \cdots + x_{k_s} + x_i)^{-\alpha} \leq (x_0 + x_i)^{-\alpha}.$$

Hence we can write

$$\begin{aligned}\mathbb{P}\left(X \subset S\right) &\leq x_0^{-\alpha} \prod_{i=1}^{r} \prod_{\substack{I \subset [r], \\ \max I = i}} (x_0 + x_i)^{-\alpha} \\ &\leq x_0^{-\alpha} \prod_{i=1}^{r} (x_0 + x_i)^{-2^{i-1}\alpha}.\end{aligned}$$

It is convenient to write $y_0 = x_0$ and $y_i = x_0 + x_i$. With this notation we have

$$\mathbb{P}\,(X \subset S) \le y_0^{-\alpha} \prod_{i=1}^{r} y_i^{-2^{i-1}\alpha}. \tag{2.50}$$

Note that if $y_r + x_1 + \cdots + x_{r-1} = \max(X) \in S_m \subset [4^{m+2}, 4^{m+2} + 4^m)$ then necessarily $y_r \le 4^{m+3}$. Hence by (2.50)

$$\begin{aligned}\mathbb{E}(N(S_m)) &\le \sum_{\substack{X=\{x_0+\sum_{i\in I} x_i \mid I\subset[r]\}\\ x_1\le\cdots\le x_r,\ \max(X)\in S_m}} \mathbb{P}\,(X \subset S)\\ &\le \sum_{y_0\le y_1\le\cdots\le y_r\le 4^{m+3}} y_0^{-\alpha} \prod_{i=1}^{r} y_i^{-2^{i-1}\alpha}.\end{aligned}$$

Taking in account that $\alpha = \frac{r}{2^r-1} + \epsilon/2$ and that $t - 2^t\alpha > -1$ for all $t \le r$ and ϵ small enough we can estimate $\mathbb{E}(N(S_m))$ as follows:

$$\begin{aligned}\mathbb{E}(N(S_m)) &\ll \sum_{y_0\le\cdots\le y_r\le 4^{m+3}} y_0^{-\alpha} y_1^{-\alpha} \prod_{i=2}^{r} y_i^{-2^{i-1}\alpha}\\ &\ll \sum_{y_1\le\cdots\le y_r\le 4^{m+3}} y_1^{1-2\alpha}\cdot y_2^{-2\alpha} \prod_{i=3}^{r} y_i^{-2^{i-1}\alpha}\\ &\ll \cdots\\ &\ll \sum_{y_t\le\cdots\le y_r\le 4^{m+3}} y_t^{t-2^t\alpha}\cdot y_{t+1}^{-2^t\alpha} \prod_{i=t+2}^{r} y_i^{-2^{i-1}\alpha}\\ &\ll \cdots\\ &\ll \sum_{y_{r-1}\le y_r\le 4^{m+3}} y_{r-1}^{r-1-2^{r-1}\alpha}\cdot y_r^{-2^{r-1}\alpha}\\ &\ll \sum_{y_r\le 4^{m+3}} y_r^{r-2^r\alpha}\\ &\ll (4^m)^{1+r-2^r\alpha}.\end{aligned}$$

Markov inequality yields

$$\sum_{m\ge m_\epsilon} \mathbb{P}\Big(N(S_m) > m^2\mathbb{E}(N(S_m))\Big) \le \sum_{m\ge m_\epsilon} \frac{1}{m^2} < \infty.$$

Thus by the Borell-Cantelli Lemma with high probability we have

$$
\begin{aligned}
N(S_m) &\ll m^2 \mathbb{E}\left(N(S_m)\right) \ll 2^{m(1+r-2^r\alpha+o(1))} \\
&\ll 2^{m(1-\frac{r}{2^r-1}-2^{r-1}\epsilon+o(1))}, \quad (m \to \infty).
\end{aligned} \tag{2.51}
$$

Combining (2.51) with (2.45) we have with high probability

$$
\frac{N(S_m)}{|S_m|} \ll 2^{m((1-2^{r-1})\epsilon+o(1))} \to 0, \quad (m \to \infty),
$$

which proves Lemma 2.14 for the $\mathcal{L}_{2,\ldots,2}^{(r)}$ case (Hilbert cubes).

Chapter 3

Palindromes in linear recurrence sequences

3.1. Introduction

Probably $F_6 = 55$ is the largest palindromic Fibonacci number. It seems, however, a hard problem to decide if there are only finitely many of these numbers. Luca proved that for any base $b \geq 2$, the set

$$\{n\colon F_n \text{ is palindromic in base } b > 1\}$$

has zero density [35]. We will use a distinct approach to prove a stronger and more general result for a broader class of linear recurrence sequences.

Theorem 3.1. *Let $b \geq 2$ be an integer and let $\{a_n\}_{n\geq 1}$ be the linear recurrence sequence of integers of minimal recurrence relation*

$$a_{n+k} = c_1 a_{n+k-1} + \cdots + c_k a_n, \qquad (n \geq 1), \tag{3.1}$$

where $c_i \in \mathbb{Z}$ for $1 \leq i \leq k$. If the polynomial $C(X) = X^k - c_1 X^{k-1} - \cdots - c_k$ has a unique dominant root $\alpha_1 > 0$ which is multiplicatively independent with b, then there exists $c = c(b) > 0$ such that

$$\#\{n \leq x\colon\ a_n \text{ is palindromic in base } b\} = O(x^{1-c}).$$

An immediate corollary is that the number of Fibonacci numbers up to x which are palindromes in any base is $O(x^{1-c})$, for some constant $c > 0$. We prove that in this case we can take $c = 10^{-11}$.

Corollary 3.1. *We have that*

$$\#\{n \le x\colon\ F_n \textit{ is palindrome in base } 10\} \ll x^{1-10^{-11}}.$$

3.2. Preliminary results

In this section, we recall several well known results that will be used in the paper. The linear recurrence sequence given by (3.1) can be *solved* as follows.

Theorem 3.2. *The general solution of* (3.1) *is given by*

$$a_n = \sum_{i=1}^{R} \alpha_i^n p_i(n), \tag{3.2}$$

where the corresponding characteristic polynomial

$$X^k - c_1 X^{k-1} - \cdots - c_{k-1}X - c_k = \prod_{i=1}^{R} (X - \alpha_i)^{\mu_i},$$

has R distinct complex roots α_i with multiplicity μ_i, and $p_i(X)$ is a polynomial of degree $\mu_i - 1$ and coefficients determined by the first k terms of the sequence $\{a_n\}_{n\ge1}$ for $i = 1, \ldots, R$.

For more details refer to [16].

We say that α_1 is *dominant* if $|\alpha_1| > |\alpha_i|$ for all $1 < i \le R$ (if a dominant root exists, we can always index it as the first one by rearranging the roots if needed). Clearly, the dominant root is real, has $|\alpha_1| > 1$ and $p_1(X)$ is a polynomial with real coefficients. In particular, the sign of a_n is the same as the sign of the leading term of $p_1(x)$ for all large n when $\alpha_1 > 0$, whereas the sign of a_n is $(-1)^n$ times the sign of the leading term of $p_1(X)$ for all large n when $\alpha_1 < 0$. Thus, by replacing $C(X)$ with $(-1)^k C(-X)$, and simultaneously changing the signs of $p_i(X)$ for all $i = 1, \ldots, R$, if needed (operations which do not change $|a_n|$ for any $n \geq 1$), we may assume that $\alpha_1 > 0$ and that a_n is positive for all large n.

Lemma 3.1. *Let M be an integer greater than* 1. *Any recurrence sequence satisfying* (3.1) *is periodic modulo M. The period $\nu = \nu(M)$ satisfies $\nu \leq M^k$.*

Proof. Consider the k-tuples $\overline{a}_r = (a_r, a_{r+1}, \ldots, a_{r+k-1})$, $1 \leq r \leq M^k + 1$. By the pigeon-hole principle, two of them are equal modulo M, say $\overline{a}_r \equiv \overline{a}_{r'} \pmod{M}$. Denote $\nu = r' - r$. Since the value of $a_n \pmod{M}$ is determined by the k previous values $a_{n-i} \pmod{M}$ for $i = 1, \ldots, k$ of the sequence, we have that the two sequences a_n, $n \geq r$ and $a_{\nu+n}$, $n \geq r$ are the same sequence $\pmod{M}$. Thus, $a_n \equiv a_{\nu+n} \pmod{M}$ for all n. □

We say that the sequence $\{s_k\}_{k\geq 1} \subset [0, 1]$ is well distributed if for any interval $I \subset [0, 1)$ we have that $D_I(y) = o(y)$ as $y \to \infty$, where

$$D_I(y) = |\#\{k \leq y : \ s_k \in I\} - y|I|| \,. \tag{3.3}$$

Write $D(y) = \sup_{I\subset[0,1)} D_I(y)$. A quantitative version of this definition is the following inequality.

Theorem 3.3 (Erdős-Turán)**.** *For any positive integer M and any sequence $\{s_k\}$*

$$D(y) \leq \frac{y}{M+1} + 3\sum_{m=1}^{M} \frac{1}{m} \left| \sum_{1\leq j\leq y} e(j\, s_k) \right|, \tag{3.4}$$

where $e(x) = e^{2\pi i x}$.

See [34, page 112] for more details.

We will write $\|x\|$ for the distance of any real number x to the the nearest integer. We say that the numbers u and v are multiplicatively independent if there do not exist integers $(x, y) \neq (0, 0)$ such that $u^x = v^y$. When u and v are positive real numbers, this condition is equivalent to the condition that the two numbers $\log u$ and $\log v$ are linearly independent over $\mathbb{Q}$.

Theorem 3.4 (Baker [3]). *For any multiplicatively independent positive real numbers y, z there exists $\delta = \delta(y, z) > 0$ such that $\|n \log y / \log z\| \gg n^{-\delta}$ for all $n \geq 1$.*

To prove Corollary 3.1 we will need to compute an explicit δ for the particular case involved. For that purpose we use the following result due to Matveev [38]. Recall that for an algebraic number η we write $h(\eta)$ for its logarithmic height given by

$$h(\eta) := \frac{1}{d}\left(\log a_0 + \sum_{i=1}^{d} \log\left(\max\{|\eta^{(i)}|, 1\}\right)\right),$$

with d being the degree of η over $\mathbb{Q}$ and

$$f(X) := a_0 \prod_{i=1}^{d} (X - \eta^{(i)}) \in \mathbb{Z}[X] \tag{3.5}$$

being the minimal primitive polynomial over the integers having positive leading coefficient a_0 and η as a root.

With this notation, Matveev proved the following deep theorem:

Theorem 3.5 (Matveev). *Let $\mathbb{K}$ be a number field of degree D over $\mathbb{Q}$, $\gamma_1, \ldots, \gamma_t$ be positive real elements of $\mathbb{K}$, and $b_1, \ldots, b_t$ rational integers. Put*

$$B \geq \max\{|b_1|, \ldots, |b_t|\},$$

and

$$\Lambda := \gamma_1^{b_1} \cdots \gamma_t^{b_t} - 1.$$

Let $A_1, \ldots, A_t$ be real numbers such that

$$A_i \geq \max\{Dh(\gamma_i), |\log \gamma_i|, 0.16\}, \quad i = 1, \ldots, t.$$

Then, assuming that $\Lambda \neq 0$, we have

$$|\Lambda| > \exp\left(-1.4 \times 30^{t+3} \times t^{4.5} \times D^2(1 + \log D)(1 + \log B)A_1 \cdots A_t\right).$$

3.3. Proof of theorem 3.1

Theorem 3.1 *Let $b \geq 2$ be an integer and let $\{a_n\}_{n\geq 1}$ be the linear recurrence sequence of integers of minimal recurrence relation*

$$a_{n+k} = c_1 a_{n+k-1} + \cdots + c_k a_n, \qquad (n \geq 1),$$

where $c_i \in \mathbb{Z}$ for $1 \leq i \leq k$. If the polynomial $C(X) = X^k - c_1 X^{k-1} - \cdots - c_k$ has a unique dominant root $\alpha_1 > 0$ which is multiplicatively independent with b, then there exists $c = c(b) > 0$ such that

$$\#\{n \leq x\colon \ a_n \text{ is palindromic in base } b\} = O(x^{1-c}).$$

It is enough to prove the estimate for dyadic intervals

$$P(x) = \{n : \ x/2 < n \leq x, \ a_n \text{ is palindromic in base } b\}.$$

For any positive integer $t = t(x)$, Lemma 3.1 yields an integer $m_t := \nu(b^t)$ which is the period of the sequence $\{a_n\}$ modulo b^t. The value of $a_n \pmod{b^t}$ is determined by the residue of $n \pmod{\nu(b^t)}$. We will write ξ_r for the residue of $a_r \pmod{b^t}$ and $\overline{\xi}_r$ for the number obtained from ξ_r by reversing digits. Hence, for $n \equiv r \pmod{m_t}$ we have that $a_n \equiv \xi_r \pmod{b^t}$. A typical sufficiently large palindromic number a_n with $n \equiv r \pmod{m_t}$ can be written in base b as

$$a_n = \overline{\xi}_r \cdots \xi_r,$$

where both ξ_r and $\overline{\xi}_r$ are strings of t digits in base b. We observe that the number of digits of a_n in base b is $\sim n \log \alpha_1/(\log b)$. The value of t will be taken at the end of the proof but certainly it will be

$$t(x) \leq \frac{\log x}{\log b} < \frac{1}{2}\#\{\text{digits of } a_n \text{ in base } b\}$$

for x large enough. Thus when $x/2 < n \leq x$ we have that ξ_r and $\overline{\xi}_r$ do not overlap. For short, we put $J = b^t$ throughout this proof. Also we define α by $m_t = J^\alpha$. Note that Lemma 3.1 implies that $\alpha \leq k$.

Since the t most significant digits of a_n are coincident with the t digits of the number $\overline{\xi}_r$, we can write

$$a_n = \overline{\xi}_r b^d(1+\theta J^{-1}), \qquad 0 \le \theta < 1, \tag{3.6}$$

for some positive integer d. By hypothesis, we know that $|\alpha_2/\alpha_1| < 1$. Thus, we have that

$$|\sum_{i=2}^{R}(\alpha_i/\alpha_1)^n p_i(n)/p_1(n)| \ll n^{\max_i(\deg(p_i))}|\alpha_2/\alpha_1|^n \ll x^{O(1)}|\alpha_2/\alpha_1|^{x/2} < J^{-1}$$

for x large enough. By Theorem 3.2, we have

$$a_n = \alpha_1^n p_1(n) + \sum_{i=2}^{R}\alpha_i^n p_i(n) = \alpha_1^n\, p_1(n)\left(1 + O\left(J^{-1}\right)\right).$$

Taking logarithms and inserting (3.6) we have

$$\log\overline{\xi}_r + d\log b + \log\left(1+\theta J^{-1}\right) = n\log\alpha_1 + \log p_1(n) + O(J^{-1}).$$

We consider first the case when the multiplicity of α_1 is $\mu_1 = 1$, so the polynomial $p_1(n)$ is a constant, say $p_1(n) = p_1$. Therefore

$$d = n\frac{\log\alpha_1}{\log b} + \frac{\log p_1 - \log\overline{\xi}_r}{\log b} + O(J^{-1}).$$

Thus, when $x/2 < n \le x,\ n \equiv r \pmod{m_t}$ and a_n is palindromic, we have that

$$\left\| n\frac{\log\alpha_1}{\log b} - \gamma_r\right\| \ll J^{-1},$$

where

$$\gamma_r = \frac{\log\overline{\xi}_r - \log p_1}{\log b}.$$

Hence, by the Cauchy-Schwarz inequality, we have

$$\begin{aligned}
|P(x)|^2 &= \left(\sum_{r=0}^{m_t-1}\#\{n\in P(x):\ n\equiv r \pmod{m_t}\}\right)^2\\
&\ll \left(\sum_{r=0}^{m_t-1}1\right)\sum_{r=0}^{m_t-1}\left(\#\left\{n\in P(x),\ n\equiv r\ \ (\mathrm{mod}\ m_t)\right\}\right)^2\\
&\ll m_t\sum_{r=0}^{m_t-1}\#\left\{n,n'\in P(x),\ n,n'\equiv r\ \ (\mathrm{mod}\ m_t)\right\}\\
&\ll m_t\#\left\{n,n'\in P(x),\ n\equiv n'\ \ (\mathrm{mod}\ m_t)\right\}.
\end{aligned}$$

We observe that if $n, n' \in P(x)$ then

$$\begin{aligned}
\left\| |n-n'| \frac{\log \alpha_1}{\log b} \right\| &= \left\| (n-n') \frac{\log \alpha_1}{\log b} \right\| \\
&\leq \left\| n \frac{\log \alpha_1}{\log b} - \gamma_r \right\| + \left\| n' \frac{\log \alpha_1}{\log b} - \gamma_r \right\| \\
&\ll J^{-1}.
\end{aligned}$$

Furthermore $|n - n'| = \ell m_t$ for some $0 \leq \ell \leq x/(2m_t)$ and, given ℓ and $n \in P(x)$, there are at most two distinct n' such that $|n - n'| = \ell m_t$. Thus, for each ℓ, the number of pairs $n, n' \in P(x)$ with $|n - n'| = \ell m_t$ is bounded by $2|P(x)|$. With these observations we have

(3.7)

$$\begin{aligned}
|P(x)| &\ll \frac{m_t}{|P(x)|} \# \left\{ n, n' \in P(x),\ n \equiv n' \pmod{m_t},\ \left\| |n-n'| \frac{\log \alpha_1}{\log b} \right\| \ll J^{-1} \right\} \\
&\ll m_t \# \left\{ \ell :\ 0 \leq \ell \leq \frac{x}{2m_t},\ \left\| \ell m_t \frac{\log \alpha_1}{\log b} \right\| \leq \frac{C}{J} \right\},
\end{aligned}$$

for some constant C. Now we use (3.3) with the sequence $s_\ell = \|\ell m_t(\log \alpha_1/\log b)\|$, the interval $I = [0, C/J]$ and $y = x/(2m_t)$. This gives

$$|P(x)| \ll m_t \left(1 + \frac{Cx}{2Jm_t} + D\left(\frac{x}{2m_t} \right) \right).$$

By Theorem 3.3, we have

$$\begin{aligned}
D\left(\frac{x}{2m_t} \right) &\ll \frac{x}{2m_t T} + \sum_{i=1}^{T} \frac{1}{i} \left| \sum_{1 \leq j \leq x/(2m_t)} e\left(ijm_t \frac{\log \alpha_1}{\log b} \right) \right| \\
&\ll \frac{x}{2m_t T} + \sum_{i=1}^{T} \frac{1}{i} \frac{1}{\|i\, m_t(\log \alpha_1/\log b)\|}.
\end{aligned}$$

As α_1 and b are algebraically independent, Theorem 3.4 yields that there exists $\delta = \delta(\alpha_1, b) > 0$ such that

$$\begin{aligned}
D\left(\frac{x}{2m_t} \right) &\ll \frac{x}{2m_t T} + \sum_{i=1}^{T} \frac{1}{i} (im_t)^\delta \\
&\ll \frac{x}{2m_t T} + T^\delta m_t^\delta \\
&\ll x^{\frac{\delta}{1+\delta}},
\end{aligned}$$

where we take $T = \lfloor x^{\frac{1}{\delta+1}}/m_t \rfloor$. We now choose

$$t = \left\lfloor \frac{\log x}{(1+\delta)(1+\alpha)\log b} \right\rfloor,$$

and then we have

$$\begin{aligned} |P(x)| &\ll \frac{x}{J} + m_t x^{\frac{\delta}{1+\delta}} \\ &\ll \frac{x}{J} + J^{\alpha} x^{\frac{\delta}{1+\delta}} \\ &\ll x^{1-\frac{1}{(1+\delta)(1+\alpha)}}, \qquad (x \to \infty). \end{aligned} \tag{3.8}$$

Now we consider the case when the multiplicity of α_1 is $\mu_1 \geq 2$. In this case, we split the interval $[x/2, x]$ in J intervals $I_j = [n_j, n_{j+1}]$ of length $\sim x/(2J)$. We observe that if $n \in I_j$ then $\log p_1(n) = \log p_1(n_j) + O(J^{-1})$. Thus, if $n \in I_j \cap P(x),\ n \equiv r \pmod{m_t}$, we have that

$$\left\| n\frac{\log \alpha_1}{\log b} - \gamma_{r,j} \right\| \ll J^{-1},$$

where

$$\gamma_{r,j} = \frac{\log \overline{\xi}_r - \log p_1(n_j)}{\log b}.$$

If we denote by $P_j(x) = P(x) \cap I_j$, we proceed as above to get that

$$\begin{aligned} |P_j(x)| &\ll m_t \# \left\{ \ell :\ 0 \leq \ell \leq \frac{x}{J2m_t},\ \left\| \ell m_t \frac{\log \alpha_1}{\log b} \right\| \leq \frac{C}{J} \right\} \\ &\ll m_j \left(1 + \frac{Cx}{2J^2 m_t} + D\left(\frac{x}{2Jm_t} \right) \right). \end{aligned}$$

As in the case $\mu_1 = 1$, we have

$$D\left(\frac{x}{2Jm_t}\right) \ll \frac{x}{2m_t T} + T^{\delta} m_t^{\delta} \ll (x/J)^{\frac{\delta}{1+\delta}},$$

therefore

$$\begin{aligned} |P_j(x)| &\ll \frac{x}{J^2} + m_j (x/J)^{\frac{\delta}{1+\delta}} \\ &\ll \frac{x}{J^2} + J^{\alpha - \frac{\delta}{1+\delta}} x^{\frac{\delta}{1+\delta}}. \end{aligned}$$

Thus,

$$|P(x)| = \sum_{j=1}^{J} |P_j(x)| \ll \frac{x}{J} + J^{\alpha+1-\frac{\delta}{1+\delta}} x^{\frac{\delta}{1+\delta}} \ll x^{1-\frac{1}{(\alpha+1)(1+\delta)+1}}$$

where we take $J \sim x^{\frac{1}{(\alpha+1)(1+\delta)+1}}$, as $x \to \infty$.

3.4. Proof of Corollary 3.1

Corollary 3.1 *We have that*

$$\#\{n \le x\colon\ F_n \text{ is palindrome in base } 10\} \ll x^{1-10^{-11}}.$$

As we said in §3.1, we now perform an effective computation of δ in Theorem 3.4 for $y = (1+\sqrt{5})/2$ and $z = 10$.

Lemma 3.2. *In Theorem 3.4, we can take* $\delta((1+\sqrt{5})/2, 10) = 4.92 \times 10^{10}$.

Proof. In Theorem 3.5, we take $t = 2$, $\gamma_1 = (1+\sqrt{5})/2$, $\gamma_2 = 10$, $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ for which $D = 2$. We can then take $A_1 = 0.5 > 2h(\gamma_1) = \log((1+\sqrt{5})/2)$, $A_2 = 4.7 > 2h(\gamma_2)$. For an integer $n \ge 2$ consider the expression

$$\|n \log \gamma_1 / \log \gamma_2\| = \frac{1}{\log \gamma_2} |n \log \gamma_1 - m \log \gamma_2|$$

for some integer m. Clearly, $m < n$, for if not the right–hand side above is at least,

$$\frac{n}{\log \gamma_2} |\log \gamma_2 - \log \gamma_1| \ge 0.79n > 1,$$

a contradiction. Thus, $m < n$. Then $B := \max\{m, n\} = n$. Put

$$z = n \log \gamma_1 - m \log \gamma_2.$$

Then

$$\frac{|z|}{\log \gamma_2} = \|n \log \gamma_1 / \log \gamma_2\| \le \frac{1}{2},$$

therefore $|z| \le (\log \gamma_2)/2 < 1.5$. Thus,

$$\frac{|e^z - 1|}{|z|} \le \frac{e^{1.5} - 1}{1.5} < 2.5.$$

We thus get that

$$\|n \log \gamma_1 / \log \gamma_2\| = \frac{|z|}{\log \gamma_2} \ge \frac{1}{2.5 \log \gamma_2} |e^z - 1| > \frac{1}{6} |\gamma_1^n \gamma_2^{-m} - 1| := \frac{|\Lambda|}{6}.$$

The right-hand side above is not zero since γ_1 and γ_2 are multiplicatively independent. We apply Theorem 3.5 to get the following inequality:

$$|\Lambda| \geq \exp\left(-1.4 \times 30^5 \times 2^{4.5} \times 2^2(1+\log 2)(1+\log n)A_1A_2\right).$$

Using the fact that $n \geq 3$, we have $1+\log n < 2\log n$, therefore

$$|\Lambda| > n^{-c},$$

where we can take

$$c = 1.4 \times 30^5 \times 2^{4.5} \times 2^2 \times (1+\log 2) \times 2 \times 0.5 \times 4.7 < 2.46 \times 10^{10}.$$

Hence,

$$\|n \log \gamma_1 / \log \gamma_2\| > \frac{1}{6} n^{-c} > n^{-2c},$$

which completes the proof of this lemma since $2c = 4.92 \times 10^{10}$. □

Now we are ready to complete the proof. The characteristic polynomial of the Fibonacci recurrence has $\alpha_1 = (1+\sqrt{5})/2$ as the unique dominant root. It has multiplicity $\mu_1 = 1$, so we can apply the estimate (3.8). It is known that for $b = 10$ and $t \geq 2$, the period of the Fibonacci sequence $\pmod{10^t}$ is $\nu(10^t) = 3 \times 10^t \ll 10^t$, so we can take $\alpha = 1$. Thus, by Lemma 3.2, we have

$$\#\{n \leq x : F_n \text{ is base 10 palindrome}\} \ll x^{1-\frac{1}{2(1+4.92\times 10^{10})+1}} \ll x^{1-10^{-11}},$$

which is what we wanted to prove.

3.5. Comments and further problems

Each of the binary recurrence sequences of general term $a_n = 10^n + 1$ or $10^n - 1$ consists of palindromes in base 10. This shows that in the case of the dominant root, the condition that the dominant root and the base be multiplicatively independent cannot be removed without affecting the conclusion of Theorem 3.1. In a related spirit, we mention that in [36], it was shown that the largest base 2 palindrome of the form $10^n \pm 1$ is $99 = \overline{110011}_{(2)}$.

We believe the conclusion of the theorem also holds under the somewhat more general hypothesis namely that the sequence is non degenerated (i.e, that α_i/α_j is not a root of 1 for $i \neq j$ in $\{1, \ldots, R\}$), and that the absolute value of the largest root of the characteristic polynomial is multiplicatively independent over b. However, we could not deal with the case when a dominant root is not present and we leave this as an open research problem.

Bibliography

[1] Ajtai, Miklós; Komlós, János; Szemerédi, Endre. A dense infinite Sidon sequence. *European J. Combin.* 2 (1981), no. 1, 1–11.

[2] Alon, Noga; Rónyai, Lajos; Szabó, Tibor. Norm-graphs: variations and applications. *J. Combin. Theory Ser. B* 76 (1999), no. 2, 280–290.

[3] Baker, A. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.* 14 1967 220–228.

[4] Ball, Simeon; Pepe, Valentina. Asymptotic improvements to the lower bound of certain bipartite Turán numbers. *Combin. Probab. Comput.* 21 (2012), no. 3, 323–329.

[5] Behrend, F. A. On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. U. S. A.* 32, (1946). 331–332.

[6] Baker, R. C.; Harman, G.; Pintz, J. The difference between consecutive primes. II. *Proc. London Math. Soc.* (3) 83 (2001), no. 3, 532–562.

[7] Brown, W. G. On graphs that do not contain a Thomsen graph. *Canad. Math. Bull.* 9 1966 281–285.

[8] Cilleruelo, Javier. Infinite Sidon sequences. *Adv. Math.* 255 (2014), 474–486

[9] Cilleruelo, Javier. New upper bounds for finite B_h sequences. *Adv. Math.* 159 (2001), no. 1, 1–17.

[10] Cilleruelo, Javier. Sidon sets in $\mathbb{N}^d$. *J. Combin. Theory Ser.* A 117 (2010), no. 7, 857–871

[11] Cilleruelo, J. and Ruzsa, I. *Real and p-adic Sidon sequences*, Acta Sci. Math. (Szegez) vol 70, no. 3-4, (1983).

[12] Cilleruelo, Javier; Tenenbaum, Gérald. An overlapping theorem with applications. *Publ. Mat.* 2007, Proceedings of the Primeras Jornadas de Teoría de Números, 107-118

[13] Cilleruelo, Javier; Tesoro, Rafael. Dense infinite B_h sequences. *Publ. Mat.* 59 (2015), no. 1, 55–73.

[14] Cilleruelo, Javier; Tesoro, Rafael. On sets free of sumsets with summands of prescribed size. *Combinatorica.* (accepted in 2015 for publication)

[15] Cilleruelo, Javier; Tesoro, Rafael; Luca, Florian. Palindromes in linear recurrence sequences. *Monatsh. Math.* 171 (2013), no. 3-4, 433–442.

[16] Everest, Graham; van der Poorten, Alf; Shparlinski, Igor; Ward, Thomas. Recurrence sequences. Mathematical Surveys and Monographs, 104. *American Mathematical Society, Providence, RI*, 2003. xiv+318 pp. ISBN: 0-8218-3387-1

[17] Erdős, P. On extremal problems of graphs and generalized graphs. *Israel J. Math.* 2 1964 183–190.

[18] Erdős, Paul; Harzheim, Egbert. Congruent subsets of infinite sets of natural numbers. *J. Reine Angew. Math.* 367 (1986), 207–214.

[19] Erdős, P.; Rényi, A. Additive properties of random sequences of positive integers. *Acta Arith.* 6 1960 83–110.

[20] Erdős, P.; Rényi, A.; Sós, V. T. On a problem of graph theory. *Studia Sci. Math. Hungar.* 1 1966 215–235.

[21] Erdős, Paul; Simonovits, Miklós. Supersaturated graphs and hypergraphs. *Combinatorica* 3 (1983), no. 2, 181–192

[22] Erdős, P.; Turán, P. On a problem of Sidon in additive number theory, and on some related problems. *J. London Math. Soc.* 16, (1941). 212–215

[23] Füredi, Zoltán. An upper bound on Zarankiewicz' problem. *Combin. Probab. Comput.* 5 (1996), no. 1, 29–33.

[24] Füredi, Zoltán; Simonovits, Miklós. The history of degenerate (bipartite) extremal graph problems. *Erdős centennial*, 169–264, Bolyai Soc. Math. Stud., 25, *János Bolyai Math. Soc., Budapest*, 2013

[25] Geneson, Jesse T; Tian, Peter M. Extremal Functions of Forbidden Multidimensional Matrices *arXiv:1506.03874v1* (2015).

[26] Green, Ben. The number of squares and $B_h[g]$ sets. *Acta Arith.* 100 (2001), no. 4, 365–390.

[27] Gunderson, David S.; Rödl, Vojtěch. Extremal problems for affine cubes of integers. *Combin. Probab. Comput.* 7 (1998), no. 1, 65–79.

[28] Halberstam, Heini; Roth, Klaus Friedrich. Sequences. Second edition. *Springer-Verlag, New York-Berlin*, 1983. xviii+292 pp. ISBN: 0-387-90801-3

[29] Katz, Nets Hawk; Krop, Elliot; Maggioni, Mauro. Remarks on the box problem. *Math. Res. Lett.* 9 (2002), no. 4, 515–519.

[30] Kollár, János; Rónyai, Lajos; Szabó, Tibor. Norm-graphs and bipartite Turán numbers. *Combinatorica* 16 (1996), no. 3, 399–406.

[31] Kövari, T.; Sós, V. T.; Turán, P. On a problem of K. Zarankiewicz. *Colloquium Math.* 3, (1954). 50–57.

[32] Lewko, Allison; Lewko, Mark. On the structure of sets of large doubling. *European J. Combin.* 32 (2011), no. 5, 688–708.

[33] Lindström, Bernt. An inequality for B_2-sequences. *J. Combinatorial Theory* 6 1969 211–212.

[34] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Dover Publications Inc., 2005.

[35] Luca, Florian. Palindromes in Lucas sequences. *Monatsh. Math.* 138 (2003), no. 3, 209–223.

[36] Luca, Florian; Togbé, Alain. On binary palindromes of the form $10^n \pm 1$. *C. R. Math. Acad. Sci. Paris* 346 (2008), no. 9-10, 487–489.

[37] Maldonado, J. *A remark on Ruzsa's construction of an infinite Sidon set* arXiv:1103.5732 (2011).

[38] Matveev, E. M. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. (Russian) *Izv. Ross. Akad. Nauk Ser. Mat.* 64 (2000), no. 6, 125–180; *translation in Izv. Math.* 64 (2000), no. 6, 1217–1269

[39] O'Bryant, K. *A Complete Annotated Bibliography of Work Related to Sidon Sequences* The electronic journal of combinatorics, DS11 (2004)

[40] Peng, Xing; Tesoro, Rafael; Timmons, Craig. Bounds for generalized Sidon sets. *Discrete Math.* 338 (2015), no. 3, 183–190.

[41] Ruzsa, Imre Z. Solving a linear equation in a set of integers. I. *Acta Arith.* 65 (1993), no. 3, 259–282.

[42] Ruzsa, Imre Z. An infinite Sidon sequence. *J. Number Theory* 68 (1998), no. 1, 63–71.

[43] Sándor, Csaba. An upper bound for Hilbert cubes. *J. Combin. Theory Ser. A* 114 (2007), no. 6, 1157–1159.

[44] Stohr A. Gelöste und ungelste Fragen der Basen der natrlichen Zahlenreihe. I, II , J. *Reine Angew. Math.* 194 (1955), 40–65, 111–140.

[45] Trujillo-Solarte, Carlos Alberto; García-Pulgarín, Gilberto; Velásquez-Soto, Juan Miguel. $B_2^{\pm}[g]$ finite sets. JP *J. Algebra Number Theory Appl.* 4 (2004), no. 3, 593–604.